ECRI NEWS
Understanding Credit Markets for Europe

CONSUMER FINANCE IN THE DIGITAL ERA

By Sylvain Bouyon
Research Fellow at CEPS-ECRI

Based on its independence and objective approach, ECRI is maintaining a strong voice on the key topic of consumer finance. In particular, we are enlarging our network of partners and deepening our expertise on key issues related to consumer finance. Through Task Forces and research projects, ECRI is playing a growing role in providing the European institutions with relevant findings in relation to the various EU policy agendas touching on retail finance. At the moment, the main dossiers covered are monetary policies, household macroeconomics and several key pieces of legislation, including PSD2, CCD, MCD, MIF, GDPR, PAD and eIDAS.

A Task Force was successfully completed in June 2018 on the best policy mix to ensure the cybersecurity of financial firms (the report can be found **here**). The main findings are being presented to different organisations, including the DG FISMA in the European Commission, and to participants in large external conferences. Another Task Force is expected to start in the last quarter of this year on "Macro-prudential and consumer protection: Two sides of the same coin?", with a focus on over-indebtedness with respect to consumer credit and housing loans.

Several ECRI research projects have been recently completed or are near completion on topics as diverse as the digitalisation of retail banks, the rules governing dynamic currency conversion, the new consumer credit Directive, data protection, financial inclusion, the drivers and remedies of consumer over-indebtedness, and the latest macroeconomic trends in relation to consumer finance. These topics are also regularly debated in conferences or workshops organised by ECRI. An especially successful conference, co-organised with CEPS and ECMI on June 7 th , was the Fintech Day. The primary objective of this all-day event was to foster a lively and informed debate on thepolicy agendas related to the GDPR, which recently became operational, the draft ePrivacy Regulation, MiFID, the eIDAS and the PSD2. This Newsletter highlights the main issues debated during the Fintech Day and the presents the points of view of key stakeholders.

As regards data protection, Nabil Hbali from Ingenico emphasises that proper compliance with GDPR and future privacy laws will require extensive technological change. Beverly Sawyers from American Express admits that in the short term the GDPR might impede certain innovations, but in the medium to long term, it should provide a foundation of trust for consumers and thereby drive innovation in this sphere. In the view of Martin Schmalzried of COFACE, not all innovations are necessarily positive, and the renewed focus on privacy and data protection should inspire additional thinking in this area.

More specifically on cybersecurity, Mark Bannon and Deborah Porret from Zurich Insurance analyse the different needs to spur cyber insurance, in particular regarding information sharing, taxonomy, attribution and responsibility, and state-backed insurance schemes. Finally, Giorgio Lorenzo Cusmà from Intesa Sanpaolo defines the main objectives for developing reinforced cybersecurity strategies, with a focus on the necessary harmonisation in regulatory requirements and the generalisation of the principles of collaboration, coordination and good communication at all levels, from the strategic vision to concrete interactions.

IN THIS NEWSLETTER

PRIVACY REGULATION AS AN ENABLER FOR FINANCIAL INNOVATION

By Beverly M Sawyers
VP, Head of Operational Excellence, American Express

Data are integral to the functioning and growth of the digital economy. The use of data analytics and artificial intelligence can help firms provide more relevant products and services to their customers and clients, as well as improve their efficiency and effectiveness.

A good example we have seen is using information about the customer and their preferences to validate that they are indeed making the financial transaction, thus reducing the burden on the customer to enter additional information whilst also delivering industry-low fraud rates.

It is also clear that consumers are being empowered in how they control their data, often driven by regulation, for example the new API rules in PSD2, and of course by wider technological innovation.

GDPR is an important framework to ensure that consumers have control over – and build trust – in how organisations are using their data. Rather than being opposed, these data protection regulations should be seen as the cornerstone of financial innovation and the data-centric models to which we are moving. The implications for businesses such as American Express are clear. Earning and securing customer trust will be key to success going forward, and how we deal with personal data will be an essential part of that.

Robust standards and practices, data protection and information security have been core to our business practices for many years, and are integrated in how we design products, services and capabilities, and in how we manage relationships with our customers. We see the new regulations as representing an evolution rather than a shakeup in terms of our relationships. Our strong foundation has enabled us to focus on not just ensuring compliance with the new rules, but going beyond that to think how we could make life easier for our customers. However, there are challenges when we look at the broader regulatory landscape, for example uncertainty over the future of the EU-UK data regime after Brexit; or interactions between GDPR and the impending ePrivacy Regulation; or indeed the practical considerations around PSD2 and TPP access to accounts.

We do not believe GDPR seriously undermines the firm's opportunity to create and deliver innovative new products and services to our customers in the long term. However, the implications need to be well understood. We have certainly found the guidance (& examples) issued by the working parties very helpful.

Picking up on specific elements, we support the right of individuals to be entitled to request their personal data to be deleted if the processing of this data is not justified. We also think it is important that businesses be required to disclose information regarding the logic involved, and consequences of the algorithms they use, especially where they might have significant impacts on consumers. From a regulatory perspective, algorithms and machine learning can't be a black box.

We also recognise that for many businesses, compliance with GDPR is creating a material work effort. In the short term there may be an impact on certain types of innovation, around cloud computing for example. But in the medium to long term, data privacy regulations provide a foundation of trust so that consumers will feel more confident sharing their data, which we strongly believe will in turn drive innovation in this space.

THINKING DIFFERENTLY ABOUT DATA PRIVACY

By Nabil Hbali
Transformation Program Manager, Ingenico Group

The EU General Data Protection Regulation (GDPR) is all about risk management, consisting of procedures and action plans to mitigate the risk of a data breach or data misuse and to empower data owners. But like any procedure or action plan to prevent something from happening, it is costly and not 100% efficient. Let's take the example of retail industry. Cash exposes merchants to the risk of theft and to robbery when cash is stored or transported. And it also exposes merchants to money laundering. To minimise these risks, retailers have made considerable investments in security equipment and measures and safe transportation services. But no matter how vigilant we are or what preventive steps are taken, we are still looking at a system with a single point of failure. The most optimal solution, therefore, would be to eliminate the source of the risk rather than the risk itself.

Indeed, since the mid-1990s, the trend in retail stores has decidedly moved away from cash payments towards more card payments. And more recently, consumers are increasingly drawn to mobile payments and electronic wallets. Further reinforcing this trend has been the drop in the number of ATMs, which had registered an steady increase until 2007.

We need to think differently if we want to guarantee data privacy. That means evolved thinking – such as removing the target and eliminating the single point of failure and putting customers fully in control of their own data. No more risk of data breach, no more customer consent, no more right to be forgotten, no more data portability…

If you look at it closer, it becomes clear that technologies bring a multitude of solutions that will make it much easier to cope with regulations. However, there is a need for regulations to catch up with the technology, for laws to adjust to the technology and for the technology to adjust to laws.

• A zero knowledge proof (ZKP) is a cryptographic technique that allows two parties (a prover and
a verifier) to prove that a proposition is true, without revealing any information about that thing
apart from it being true while still protecting the user's privacy.
• With blockchain technology, the information is encrypted and isolated on end-user devices,
verified against itself, with public-key cryptography providing the communication channel to the
service provider.
• Under PSD2, banks should obtain the consent of their customers to allow them to share their
payment account information with third-party providers, which actually match perfectly with
the right to data portability introduced by GDPR.

It's difficult to forecast precisely how, but GDPR will enable new innovations and new services. Plenty of companies with their head in the sand are quite content to do the same thing year after year. Those companies will die off in the next five to ten years. Once customers know that better alternatives exist, the tipping point becomes inevitable.

Finally, if both technologies and the GDPR fail to align, Europe could find itself closed off from the future
of the internet to its own detriment.

PROTECTING PRIVACY WHILE PRESERVING INNOVATION: AN IMPOSSIBLE GOAL?

By Martin Schmalzried
Policy and Advocacy Manager, COFACE – Families Europe

As technology advances at a fast pace and permeates into every industry, the financial sector is undergoing strong changes, especially in the ever growing use of data, including highly sensitive data, to propose innovative and 'tailored' financial products. At the same time, we have seen increased focus on the rights to privacy and data protection as consumers, financial services users and regulators start seeing some worrying consequences of artificial intelligence, algorithms and data analytics, including the risk of discrimination and social exclusion. Can we reconcile innovation with the respect of certain key principles such as the right to privacy?

Innovation is not necessarily positive. All too often, innovation is systematically presented as a 'good' thing, but there are plenty of examples of harmful innovation. Regulation, far from being a burden, can save consumers, citizens, public authorities and even financial institutions from major problems. The most salient example is the 2008 financial crisis which saw major 'innovations' in the form of subprime lending, securitisation (mortgage backed securities) and credit default swaps, which proved to be toxic and the effects of which are still felt today. A more recent example is the dynamic currency conversion service, which, far from providing consumers a useful service (paying in their national currency abroad), adds a significant surcharge to the consumer. Finally, several European countries including Belgium have interest rate caps, making it very hard if not impossible for pay day lenders to enter the market with their innovative financial products. Yet nobody seems to find this problematic.

Who are you innovating for? Ideally, innovations should benefit everyone and should be a win-win, but all too often, innovations mostly benefit shareholders and aim at increasing profitability without necessarily providing some equivalent added value to consumers. Another important factor is examining the impact of innovation on financial inclusion. If your financial service only benefits the richest and least vulnerable consumers and increases the vulnerability or exclusion of the most fragile elements in our society, then it cannot be seen as 'positive'.

Good innovations do exist. There are examples of positive innovations to be sure, in the field of financial services and in Fintech. In most cases, Fintechs focus on doing in a faster/cheaper/better (more intuitive and user-friendly way) what traditional banks have been doing so far (credit, insurance, payments, investment). One example is Transferwise which enables the transfer of money across borders and especially in foreign currency at a fraction of the cost using more 'traditional' means like a bank transfer.

The transformative power of the GDPR. There are a few key provisions which, inside the GDPR, have the potential to transform the financial services industry, and especially the Fintech sector. Those principles are: data minimisation, data portability, objection to automatic decisions made by algorithms, transparency of algorithms, and purpose limitation (the principle of only collecting the strictly necessary data for the purpose of delivering a specific service). Taken together, they could usher in a new era in which consumers are in charge of their own data directly (host their own data on the cloud service of their choice) and grant access to services based on their preferences. This could greatly facilitate bank account switching for instance, as it would only require changing which financial service provider has access to their transactions history and other relevant data. Purpose limitation on the other hand is absolutely essential to avoid a race to the bottom where any and all consumer data are used in insurance and credit risk assessment, leading to the end of risk pooling and moving towards personalised risk-based pricing. Regulators will have to clarify what data is strictly necessary for carrying out creditworthiness assessments or assessing risk for various insurance policies (health insurance, car insurance, etc.), ensuring a balance between personal responsibility and risk pooling. Also, the GDPR may prompt businesses, especially those operating online, to diversify their business models and move away from the dependency on exploiting user data for targeted advertising. Examples include crowdfunding and online donation via facilitated online micro-payments, or in browser cryptocurrency mining.

Privacy in the age of mass manipulation. If the Cambridge Analytica scandal taught us anything, it is not so much about privacy violations, which have been numerous throughout the past, but about the wider negative consequences of privacy violations (mani-pulation during elections), which up until then had been limited to personal detriment. The importance of privacy and data protection goes beyond the issues of personal data breaches and individual consumer detriment, but can have deep implications for democracy. The protection of sensitive data such as financial data should, in this regard, be of utmost importance, and not relegated to questions of 'stifling innovation'.

To conclude, the GDPR and a renewed focus on privacy and data protection may allow us to move from a mentality of 'moving fast and breaking things', something that was a part of Facebook's internal 'mantra' for their staff, to 'moving slow and fixing things', stopping to think about the implications of what we are creating rather than being the first to push it on the market, regardless of wider societal implications.

ECRI STATISTICAL PACKAGE 2017

For the second time, detailed data on several "emerging economies".

Since 2003, the European Credit Research Institute (ECRI) has published a highly authoritative, widely cited and complete set of statistics on consumer credit in Europe. This valuable research tool allows users to make meaningful comparisons between all 28 EU member states as well as with a number of selected non-EU countries, including the US and Canada.

WHAT IS COVERED?

Two Statistical Packages are on offer. The more compre hensive product "Lending to Households (1995-2016)" contains valuable data on consumer credit, housing loans, other loans, total household loans, loans to non-financial corporations as well as total credit to the non-financial business and household sector. The 'standard' "Consumer Credit in Europe (1995-2016)" exclusively covers consumer credit data.

The 2 Packages in Fact & Figures:

- 40 Countries: EU 28, Turkey, Rep. of Macedonia, Iceland, Norway, Switzerland, Liechtenstein, Australia, Canada, Japan, the United States, India and Russia, Mexico and Saudi Arabia.
- 21 years data series: 1995-2016
- National accounts: GDP, final consumption expenditure and gross disposable income of households, inflation and exchange rates.
- 150 (67) tables: present time series data in nominal and real terms, and per capita, as well as breakdowns by lender, type, currency and maturity are also available for selected countries.
- 27 (13) figures: highlight credit trends in a way that allows user to make meaningful comparisons of the retail credit markets across countries.

FACTSCHEETS

The European Credit Research Institute (ECRI) provides indepth analysis and insight into the structure, evolution and regulation of retail financial services markets in Europe. Through its research activities, publications and conferences, ECRI keeps its members and the wider public up-to-date on a variety of topics, such as retail financial services, credit reporting and consumer protection at the European level.

For further information, contact Sylvain Bouyon at sylvain.bouyon@ceps.eu or at +32 (0) 2 229 39 87 87

WHAT'S NEEDED TO SPUR CYBER INSURANCE?

By Mark Bannon
Head of Cyber Liability, EMEA, Zurich Insurance

Cyber insurance is a key component of cyber resilience. Despite its fast growth in Europe, the cyber insurance market is not yet a mature market. In fact, it's still in its infancy. Zurich believes that four key elements must be tackled to enable the development of the cyber insurance market:

Information sharing. The lack of data and data sharing on attempted or actual cyber incidents is the key element limiting the underwriting of cyber insurance. Data availability would allow us to simulate the accumulation of risk, as well as to define an appropriate risk premium and foster awareness and resilience. The European Commission must be more ambitious in tackling this important issue, and soon.

Moreover, incident reporting should be required across all industry sectors. Unfortunately, we note that the GDPR guideline on personal data breach notification neither promotes centralised information sharing, nor does it contain the pertinent data to be reported from the perspective of cyber-insurance underwriting. The Geneva Association (GA, an international 'think tank' specialising in strategically important insurance and risk management issues) is promoting the development of a cyber-incident data repository, based on an adapted 2016 pilot project of the Chief Risk Officers' Forum and its taxonomy. As a start, some GA members would report cyber breaches experienced by their clients in full compliance with data privacy requirements on an anonymised basis. The objective would be to gain experience and establish a meaningful reporting framework to be used by the underwriting community in order to develop the cyber insurance market.

Taxonomy. Fragmentation in the taxonomies of cyber incidents needs to be reduced. It is important to develop a common global taxonomy, which has the ability to evolve. For this, we need the support of policy-makers. As reported in the CEPS-ECRI report, high fragmentation can be observed as regards to rules in taxonomy for reporting, reporting time frames, the template to be used and the threshold to trigger an incident. This is an issue, given that cyber-attacks do not respect national borders and different regulatory reporting requirements are emerging with increasing frequency (e.g. GDPR, the NIS Directive and PSD2). There are different possibilities to proceed: CEPS recomends agreement at EU level on a small set of common taxonomies for specific use cases. The CRO Forum developed a methodology for a common cyber risk categorisation to promote the capturing of data on cyber incidents (incidents both leading to losses as well as near misses) and to raise awareness and understanding of cyber exposures. Other institutions, such as the OECD and FSB, are also working on this.

Attribution & responsibility. For the purpose of cyber insurance underwriting, attribution is key - designating who committed the attack. Generally, attribution of cyber-attacks is not straightforward. It often results from a complex, costly and lengthy process, involving external experts and authorities. Some attacks are uncovered late. And even if attribution is possible, cyber-attacks perpetrated by organisations connected to – and funded by – nation states sometimes cannot be prevented, due to their level of sophistication. Implementation of measures to prevent IP masking would be very helpful in addressing attribution of a cyber attack[1]. In addition, better detection, prevention and more efficient combatting of all forms of cybercrime on a national, regional and global level are required. Zurich has worked with the World Economic Forum to create the foundation for public-private cooperation in fighting cybercrime. Through this initiative, we hope that alliances can be created.

Stat- backed insurance scheme - Large accumulation and/or aggregation risks are of significant concern. Loss events could reach such a large scale that they may be beyond the capital base of private insurance carriers. This is relevant to cyber events such as cyber terrorism, i.e. cyber-attacks on national critical infrastructure such as power grids, public transport (road, rail, sea and air transport), stock markets, central banks, etc.For now, insurers can cope with the present premium volume. Given the high demand and expected market growth, however, consideration should be given to government-backed insurance schemes similar to those existing for natural disasters. Given that the cyber insurance market is not yet established, defining the set-up of state-backed funds is challenging. The respective roles of insurers, reinsurers and governments should be clarified. Improved data should help inform the parties of where the respective limits would need to lie.

Zurich welcomes the European Commission's adoption of cyber security as one of its priorities. We look forward to further engaging with EU stakeholders; to help contribute to and tackle some of the key issues and to further develop the cyber insurance market.

---

1 See Larry Greenemeier, "Seeking Address: Why Cyber Attacks are so Difficult to Trace Back to Hackers", Scientific American, 11 June 2011 (https://www.scientificamerican.com/article/tracking-cyber-hackers/).

RECENT PUBLICATION

Research Report: Cybersecurity in Finance: Getting the policy mix right!
Authors: Sylvain Bouyon, Simon Krause

For more information, visit our website ***www.ecri.eu***

DIGITAL TRANSFORMATION AND CYBERSECURITY: INNOVATIVE EVOLUTION, REGULATORY PROTECTION AND ENHANCED RESILIENCE

By Giorgio Cusmà Lorenzo
Head of Information Security Business Continuity Governance, Intesa San Paolo

George Orwell introduced a concept that is at the centre of GDPR concerns today when he wrote "1984" in 1948: BIG BROTHER IS WATCHING YOU. Orwell was a visionary mind able to think about a constant monitoring of everybody actions, even though at that time television in UK meant a bulky household appliance transmitting the BBC's black and white broadcasts and ARPAnet, the Internet forerunner, was yet to come. It is worth highlighting that Orwell had identified the risks associated with the new futuristic technologies and the impact that these could have on the "rights and freedoms of natural persons" (§. Art.35 GDPR). 70 years later, this is still one of the key risks requiring mitigation and protection under the EU's regulatory framework.

Digital transformation has led to a highly interconnected environment, with unprecedented opportunities to review business paradigms and operating models, new opportunities arising from technological innovation that were not identified in Orwell's dystopic view. We cannot stop the evolution and we cannot even imagine going back into the past to protect ourselves and adopt a risk avoidance strategy. Since avoiding the digital eco-system is not an option, we need to find the right balance between innovation and protection, and to identify the best or most powerful means of coping with cyber risks.

Digital transformation in the financial Sector has created a paradigm shift in traditional business models. Digital banking in the EU Digital Single Market and beyond it have introduced new rules: the final users are acting as payment initiators through multiple channels and new players are offering payment initiation services, which are often integrated into e-commerce platforms. These evolutions have introduced issues related to the Strong Customer Authentication, to fraud detection and to the security of internet-based transactions. Another feature of the digital economy is that it is highly interconnected and borderless. Cybersecurity therefore requires an holistic vision to leverage new opportunities arising from innovative technologies, while adopting mitigation approaches to cyber-risks and also taking processes, cultures and related needs for awareness and education into consideration. Interconnected devices and processes generate a continuous flow of data exchanges across the digital ecosystem. **The availability of a huge amount of data is a key element in the digital ecosystem, representing:**

- A great opportunity to offer more tailored services to customers by leveraging data analytics;
- A significant asset to be protected against cyber criminals, and to handle in respect of data protection regulatory requirements;
- A powerful source for developing analysis and knowledge about cyber-attacks and the evolution of their patterns in order to undertake countermeasures.

From a cyber security standpoint, big data has introduced new possibilities in terms of analytics and security solutions to protect data and prevent potential cyberattacks. However, meanwhile it has also given cyber criminals the opportunity to access huge quantities of sensitive and personal information using advanced technologies.

Big data generates more opportunities arising from data mining and data analytics to generate valuable and marketable information (e.g. under PSD2), while creating a larger and often distributed base of assets to protect under the bank responsibility. There is therefore the need to combine new technologies and new collaborative organisational models to exploit the potential of predictive analysis. In this respect it is worth exploring how artificial intelligence could generate value to develop faster and more efficient algorithms and patterns evolution. High-performance computing applied to cryptography, encryption and decryption algorithms, along with artificial intelligence, are technological means to be adopted in the cyber-fight. Criminals are more and more structured and organised, and the 'good guys' in charge of cybersecurity need to become at least as organised as they are, considering that the speed of innovation is unprecedented and that each innovative solution will represent a double-edged sword, making cyber-security a moving target or enabling an ongoing approach to an ever-changing landscape.

It is therefore important to acknowledge that both the public and private sectors have recognised that the cybersecurity challenge will be critical for a very long time. In this respect, to protect the Digital Single Market, EU institutions and supervisors have introduced a wide set of regulations, ensuring that cyber-security is not only a relevant matter, but also a compelling need with the introduction of mandatory regulatory requirements and compulsory milestones. With the Cybersecurity Act and the "Coordinated Response to Large Scale Cybersecurity Incidents and Crises" Blueprint, the EU institutions have also identified the need for better coordination under some institutional guidance. More recently, the EU and other international institutions, along with FMIs and other key stakeholders have recognised that the next stage will be to harmonise regulatory requirements, which would be more efficient than the fragmented regulatory environment arising from different national or sectoral perspectives. Cybersecurity is indeed borderless and cross-sectoral as is recognised by the NIS Directive.

Continuously evolving regulatory requirements are not enough to achieve enhanced cyber-resilience. It is of utmost importance to foster dialogue between institutions and private stakeholders. The keywords are collaboration, coordination and communication, at all levels from strategic vision to concrete interactions. In the financial industry, the private sector has a long tradition of cooperation and information sharing. In order to foster cyber-resilience, these approaches have recently been applied to cybersecurity, and ongoing initiatives are looking into the best ways to leverage incident reporting, not only as a mandatory regulatory requirement, but also as a source of knowledge to be shared, upon appropriate anonymisation, along with the vulnerabilities identified either by the financial institutions or by their partners along the supply chain. The

preventive approach is key to enhancing cyber resilience. Nowadays, cyber criminals are well trained and organised, so no one can predict the breadth and the potential damages that a large scale cyber-attack could cause. In this respect, the readiness to respond to an incident is vital to guarantee business continuity by avoiding or at least minimising disruptions and associated financial losses.

The preventive approach should encompass four major areas:
• Foster collaboration among all cybersecurity stakeholders to promote sharing of knowledge that is useful for reacting properly and promptly;
• Undertake EU cyber-exercises that simulate large-scale incidents or crises;
• Set up widespread education and awareness programmes in order to be prepared to at least the same degree as cyber criminals are and to understand better how to mitigate potential threats. Education programmes should involve all employees so as to cover the human factor and influence their behaviour. Specific training should be available to all cyber experts to keep them updated on the most recent threats and mitigation procedures;
• Invest in new technologies such as artificial intelligence, machine learning, quantum computing, and in new operational patterns such as Threat Intelligence Platforms, ISACs and common application features. The combination of new technologies and new info-sharing arrangements should provide an opportunity to gather more information and data, thereby enhancing capacity to better analyse big data on threats and anomalous behaviours and leading to improved readiness.

Collaboration, coordination and communication have also been identified as pillars within the EU Cyber Security Strategy. They are unquestionably relevant when it comes to responses to cyber-incidents and are highly valuable in a preventive approach. And that is why we should all be investing resources in this approach to make the digital ecosystem more cyber-resilient.

CORPORATE MEMBERS

BNP PARIBAS PERSONAL FINANCE

ING BANK

International Personal Finance

PFG | Provident Financial Group

schufa

VISA

ACI payment systems

AMERICAN EXPRESS

Cofidis

ASSOCIATE MEMBERS

Sparda-Bank freundlich & fair

ABBL

DLA PIPER