ECRI NEWS
Understanding Credit Markets for Europe

PRIVACY RIGHTS, CYBERSECURITY AND OVER-INDEBTEDNESS IN THE MENU

By Sylvain Bouyon
Research Fellow at CEPS-ECRI

25 th May 2018 is the deadline for the implementation of the General Data Protection Regulation (GDPR) and the e-Privacy Regulation, two key pieces of legislation that have the potential to significantly change practices in the retail banking sector regarding privacy rights. Proper and efficient use of personal data remain at the core of the delivery of well-designed financial services to consumers. As such, GDPR and e-Privacy can markedly affect the different stages of products such as consumer loans or mortgage loans: marketing, advice, scoring, recovery, etc.

This is the background for "Big Data, innovation and regulation in finance: finding the right balance!", the Fintech annual conference ECRI is organising in partnership with ECMI. Held on 7 June in Brussels, the event will try to assess how and to what extent both financial innovation and consumer rights can be promoted. It will also address the different issues involved in enabling the development of balanced processes for robo-advisers. Last but not least, this conference will look closely at cybersecurity in finance and the most adequate policy mix to address the growing problem of cyber-attacks. To tackle that subject, we are pleased to welcome the Executive Director of ENISA, Udo Helmbrecht.

Cybersecurity in finance is a particular focus for ECRI and it has brought a group of experts from the financial industry together in a Task Force on cybersecurity in finance since September 2017. The original purpose was to debate the multi-sectoral cybersecurity package adopted by the European Commission in September 2017, and to build specific policy recommendations that can contribute to strengthen the cyber resilience and response of EU financial firms. Key findings of this initiative will be presented at the Conference on 7 June, but Task Force Chairman Mr Richard Parlour already outlines some elements in this Newsletter. Additional reflections are provided by Rasmus Theede, an expert with an experience of twenty years working with international security management.

Still on the digital agenda of banks, ECRI recently published a study commissioned by ACI Worldwide, "Costs and values in banks: a model fit for the digital area?". An event was organised on 12 April to discuss the multi-dimensional aspects of the digital transformation of both retail and corporate banks, and what positions policymakers should take on these issues. The main findings and the related executive summary of the study are republished in this Newsletter. Further initiatives by CEPS and ECRI are expected during the coming year on the best policy approaches to stimulate a balanced digitalisation of banks.

In the second half of the year, ECRI will be organising specific initiatives to contribute to the increasing debate about how financial education can contribute to decrease households' over-indebtedness. Other policy tools aimed at addressing the issue of over-indebtedness will also be discussed. To gain a better understanding of what is at stake, ECRI will place specific focus on the latest progress in the research that analyses the drivers behind the dynamics of over-indebtedness.

IN THIS NEWSLETTER

Privacy rights, cybersecurity and over-indebtedness in the menu Sylvain Bouyon, p. 1

Is EU on the way to building a castle of paper security?, Rasmus Theede, p. 2

Cybersecurity in the EU Financial Sector, Richard Parlour, p. 3

ECRI Membership Information, p. 2
ECRI Statistical Package 2017, p. 3
ECRI Upcoming Events, p. 4
ECRI Publications, p. 4
ECRI Members, p. 5

Understanding Credit Markets for Europe

IS EU ON THE WAY TO BUILDING A CASTLE OF PAPER SECURITY?

By Rasmus Theede
Managing Partner, DigitalNations

As May 25, the long-awaited "GDPR Day", is approaching fast, let me already share a few reflections on what I have experienced and how it has impacted cyber security in Europe.

Out of my 20 years working with international security management, the last two years have been unique. I have never seen so much focus on privacy and information security, so much work done, so many improvements in companies of all sizes and, let's not forget, so much pain, confusion, paperwork, legal arguments and diversified perceptions of what to do. As a security professional by heart, I was a strong supporter of legislation like the GDPR from the beginning. I have however become sceptical along the way and, perhaps, ended up being a bit cynical about what I have seen.

Good things first: without any doubt, the general security level of almost all companies I have worked with has increased significantly. In particular, the threat of heavy fines (few talk about the opportunities) has finally roused company management into making much-needed investments. GDPR has forced companies to clean up their data, think of new ways of handling and collecting (or not collecting) information. Quite a few companies I have worked with have fully embraced the concepts and implemented smart GDPR functions into their products and services, giving people new possibilities for discovering the way their data is handled, processed and stored. It is clear that GDPR has brought about the biggest breakthrough in both privacy protection and information security ever.

But the road to get here has been far from pretty, unnecessarily complex, confusing, expensive and frustrating and is a perfect example of "In theory, theory and practice are the same. In practice they're not". Especially for small and medium-sized companies: in an unfair game, they have been thrown into the hands of expensive lawyers, consultants and security salespeople, with very few practical guides on what to do. And even now, a few weeks before "G-day", lawyers and experts are still arguing how to interpret the new rules. With the implementation of GDPR, the operation may have been successful (time will show), but the patient nearly died. And, I think, few will argue that we ended up with a unified European approach to Data Protection in the end. On the contrary, the GDPR has been fragmented by national interests, lobbying and an academic approach to solving practical problems. As a security professional, I will argue that the GDPR has been 33% actual data protection, 33% paperwork and 33% complete confusion.

Putting positive glasses on again, as I will, I hope that regulators will now just take the time to stop, reflect and gather data before we see another such impactful and resource consuming attempt at regulation. Let the GDPR operate, adjust where needed and work with real-life companies in the field to gather experience. And I hope that the process of how the GPDR went from initial idea to final implementation is closely analysed and considered in further regulation like the ePrivacy, certification schemes and all the other new exciting initiatives in the pipeline.

Personally, my money and efforts will be on where we can get most value (meaning privacy, security and not forgetting business) for the least effort. The missing cyber hygiene controls that are responsible for by far the most data breaches, the European cross-border knowledge sharing that is so important to allow us to fight cybercrime effectively and, last but not least, practical guidance for companies and citizens. Let's stop, reflect and do the hard work. Otherwise, I fear that Europe will be well on the way to building a majestic castle of paper security.

Understanding Credit Markets for Europe

LACK OF TRANSPARENCY IS BIGGEST DRIVER OF COST

By Richard Parlour
Financial Markets Law International, Chairman EU Task Force on Cybersecurity Policy for the Financial Sector

With the rise and rise of e-commerce comes the rise and rise of the e-criminal. Cybercrime is now the world's fastest growing crime. It has leapt to number two of the top ten business risks worldwide, from not even appearing in that list five years ago. For certain countries, cyber attack is now the risk of greatest concern. Gone are the days of concern about a low level hack of a website by a script kiddie. Today's attackers are multi-faceted and increasing in sophistication, ranging from advanced persistent threats, corporate espionage, organised crime, and hactivists to cyberterrorists. Cybersecurity has moved from being a technical issue to a political and boardroom issue. Financial markets are particularly important as they oil the wheels of all EU member state economies.

In that context, ECRI has organised a Task Force with experts from financial firms to provide a list of key recommendations aimed at reinforcing cybersecurity in the EU. As the Task Force was debating the above strands, the following issues have also arisen:

- Fragmentation in the taxonomies of cyber incidents, which needs to be reduced;
- Significant initiatives need to be taken to improve the efficiency of the legislative and institutional framework for incident reporting;
- Ambitious policies are needed to develop consistent, reliable and exploitable statistics on cyber trends;
- Authorities should assess how and to what extent a centralised incident database should be shared with supervisors, regulators, firms and clients;
- Best practices for cyber-hygiene should be continuously enhanced by regulators and supervisors;
- Certification systems need careful planning if they are to be effective;
- In order to improve general efficiency and effectiveness, reinforcement of cross-border cooperation and legal convergence remains a priority;
- Policy-makers should further assess the costs, benefits and feasibility of creating an emergency fund in case of crippling cyber attacks.

A combination of the above entails the concept of cybersecurity being replaced by the concept of cyber resilience. May I strongly encourage you to read our Task Force report after its release on 7 June, and more importantly, act upon it.

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

Upcoming Event

DATA, INNOVATION & REGULATION IN FINANCE: FINDING THE RIGHT BALANCE!

07 June 2018 | Place du Congres 1, 1000 Brussels

The pace of data-driven innovation is accelerating in financial services. The promise of benefit for both firms and clients will become reality as long as the right policies and enablers are in place. To help meet that challenge, CEPS, ECRI and ECMI are jointly organising their Annual Fintech Conference on "Big Data, Innovation and Regulation in Finance: Finding the right balance!"

Given the significant impact of digitalisation on all types of products and clients, the objective of this conference is to provide a platform for the exchange of good practices across the various supervisors and providers of financial services, thereby contributing to greater regulatory consistency across the different segments of financial services. As such, the scope is relatively wide and intends to include retail financial services (credit, savings and payments), as well as investments and insurance. The programme features key stakeholders in the financial services sector and high-level representatives from the European institutions, national authorities, the financial industry, FinTech start-ups and academia.

The conference will first explore the interplay between data privacy rights and financial innovation. It will then discuss the potential benefits, risks and challenges for robo-advisors and the capacity to progress from niche markets to the mainstream. The debate will finally explore how policy-makers could further help financial firms better protect critical data against increasingly complex cyber-attacks.

Join us by registering here.

Recent Publications

COST AND VALUE IN BANKS: A MODEL FIT FOR THE DIGITAL ERA?

By Sylvain Bouyon
CEPS-ECRI

Retail and corporate banks have to cope with legacy issues that impede their efficiency and reactivity. In particular, different norms within groups are still used for accountancy, cost allocation systems and product hierarchies. Also, the share of IT spending used to maintain existing IT systems remains high. Yet, many of the banks' activities are being rapidly digitalised, especially in consumer finance. The potential of data analytics is being gradually unleashed at different stages of the products. In that context, regulators should favour the digitalisation of banks while alleviating related risks. They should also build on this mutation to raise consumers' welfare and the competitiveness of non-financial corporations (NFCs). Among these measures, the treatment of certain software expenses in the new Capital Requirements Regulation could be reassessed. Also, authorities should better foresee the cost of IT changes needed for implementing new rules and the indirect impact of those rules on banks' clients, especially SMEs. Further convergence in know-your-customer processes for NFCs is needed. The preventive approach in credit should be generalised to all clients. Finally, labour and education policies are key to ensuring a sufficient supply of IT skills.

Download publication here.

DYNAMIC CURRENCY CONVERSION AND CONSUMER PROTECTION: FINDING THE RIGHT RULES

By Sylvain Bouyon and Simon Krause
CEPS-ECRI

The growing choice of payment services should be good news for consumers, but only if they have complete information about the products being sold and the prices charged by each firm.

Several policy options are under discussion for better regulation of the dynamic currency conversion (DCC) payment service, each of which offers specific advantages but also poses distinct challenges. Enhancing trans parency, for example, will require creative solutions. The imposition of fixed price caps would call for the design of robust criteria to determine the level of the caps. And the adjustment of the payment card chip would necessitate the adoption of common standards between card providers. From a consumer protection perspective, a ban on DCC makes sense only if all other options have been exhausted and if consumers can find satisfactory alternatives. Overall, despite the challenges it presents, the first option – enhancing transparency – is the most promising. The mandatory disclosure of an indicative spread seems to be the best way for most consumers to truly understand what is at stake and how much they are paying for what.

Download publication here.

Corporate Members

BNP PARIBAS Personal Finance

ING BANK

International Personal Finance

PFG | Provident Financial Group

schufa

VISA

COFIDIS

AMERICAN EXPRESS

Associate Members

Sparda-Bank freundlich & fair

ABBL

DLA PIPER