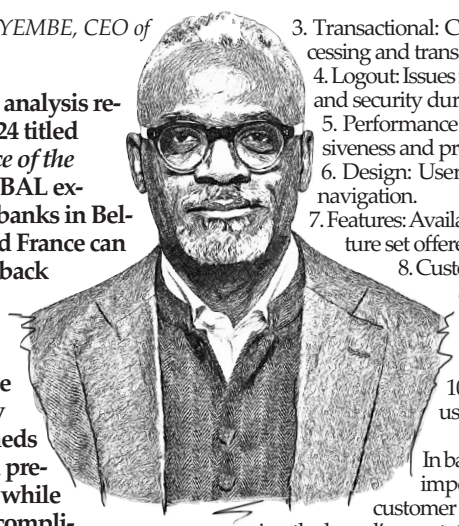
Enhancing customer experience through a risk & compliance-based approach

By Michel KABANGA KAYEMBE, CEO of 3nity-global.com



In the latest research analysis released in August 2024 titled *Optimizing the Voice of the Customer*, 3NITY GLOBAL explores how traditional banks in Belgium, Luxembourg, and France can leverage customer feedback from social media and web channels to refine their mobile app user experiences. Beyond the sentiment expressed by users, the report also sheds light on how this could preserve brand reputation while detecting areas of non-compliance with key regulations such as PSD2, DORA, and GDPR.

Importance of friction and its role in the user journey

The analysis is based on data fed into a proprietary AI-driven customer experience analytics platform, KAM-XF. The platform transforms user testimonials into valuable insights, enabling banks to address friction points that hinder the user journey and sustain their competitive edge. Friction was defined based on 10 categories depicting the user journey, with underlying subcategories starting from onboarding through platform stability, design, features, and overall user satisfaction. These categories included:

1. Onboarding: Issues related to account setup and authentication.
2. Platform Reliability: Service disruptions and technical errors.
3. Transactional: Challenges with payment processing and transaction validation.
4. Logout: Issues related to session management and security during logout.
5. Performance (Speed): Application responsiveness and processing speed.
6. Design: User interface design and ease of navigation.
7. Features: Available functionalities and the feature set offered.
8. Customer Support: Responsiveness and quality of support.
9. Security & Privacy: Data protection and privacy concerns.
10. Overall Satisfaction: General user experience and sentiment.

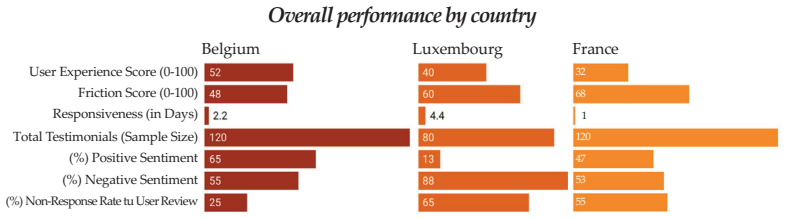
In banking apps, friction is critically important as it directly impacts customer satisfaction, potentially harming the brand's reputation or influencing other users positively. A frictionless experience ensures that users can perform transactions smoothly, access information quickly, and receive support without delay—essential factors for maintaining a competitive advantage.

Institutional performance by country

The paper reveals significant disparities in user experience across Belgium, Luxembourg, and France within the retail banking sector, emphasizing the importance of addressing friction points and improving responsiveness.

- **Belgium** leads with a user experience score of 52/100, showcasing moderate user satisfaction, although there's room for enhancement. The friction score is relatively low at 48/100, indicating fewer obstacles in the user journey. The responsiveness in addressing user issues is commendable, with an average of 2.2 days. Positive sentiment is strong at 65%, though 55% of the feedback is still negative. The non-response rate stands at 25%, suggesting a relatively proactive approach to user feedback.
- **Luxembourg** shows a lower user experience score of 40/100, with a high friction score of 60/100, reflecting more significant barriers in the user journey. The responsiveness is slower, averaging 4.4 days, and the positive sentiment is notably low at 13%, while negative sentiment is overwhelming at 88%. The non-response rate is also concerning at 65%, indicating a less effective response to user reviews.
- **France** presents a mixed picture with a user experience score of 32/100, the lowest among the three countries. The friction score is the highest at 68/100, pointing to substantial obstacles in the user journey. However, France outperforms in responsiveness, with an average of 1 day, reflecting quicker responses to user issues. Positive sentiment is moderate at 47%, with a corresponding 53% negative sentiment. The non-response rate is 55%, showing room for improvement in addressing user feedback.

Overall performance by country



These insights highlight the critical need for financial institutions in these regions to focus on reducing friction, improving responsiveness, and actively engaging with customer feedback to enhance overall user experience and satisfaction.

Regulatory risks

The white paper identifies key regulatory risks that could arise from user experience issues:

1. **PSD2:** Payment processing delays and validation errors could lead to non-compliance with the Payment Services Directive 2 (PSD2).
2. **GDPR:** Data handling issues, such as improper logout processes and security flaws, could result in breaches of the General Data Protection Regulation (GDPR).

DORA: Frequent crashes and slow performance .3 pose risks under the Digital Operational Resilience Act (DORA), potentially leading to operational .disruptions

KAM-XF's unique offering

KAM-XF is a new entrant in the customer experience analytics market, offering a unique value proposition. Unlike existing platforms, KAM-XF provides digital risk assessments that evaluate not only reputational risks but also exposure to regulatory risks such as PSD2, GDPR, and DORA. This capability makes KAM-XF a crucial tool for financial institutions looking to protect their brand, ensure compliance, and enhance the user experience.

Way Forward

The white paper suggests a proactive approach for financial institutions to continuously monitor and improve the user journey. By addressing identified frictions through the KAM-XF platform—or by adequately utilizing an existing customer experience analytics platform—banks can enhance customer satisfaction and mitigate regulatory risks. Continuous improvement, with a strong focus on customer experience, is crucial to staying competitive in the rapidly evolving digital banking landscape.

Payments Forward: Understanding PSD3 and PSR

By Oriane KAESMANN, Research Manager the LHoFT

In June 2023, The European Commission unveiled two significant legislative proposals: the third Payment Services Directive (PSD3)[1] and the Payment Services Regulation (PSR)[2]. These updates are designed to replace the existing framework under PSD2, which has been in place since 2015. PSD3 and PSR aim to modernise and strengthen the regulatory environment for payment services across the European Union, ensuring that it keeps pace with the rapid advancements in digital finance. These texts introduce crucial changes that will shape the future of innovation, competition, and security in the payment service industry.

By tightening regulatory oversight, enhancing consumer protections, and enabling a more competitive landscape, these proposals will both address current challenges and set the stage for the next wave of Fintech evolution.

Key Changes and Innovations

Merging of E-Money and Payment Services

One of the most significant updates is the merging of the E-Money Directive with the Payment Services Directive[3]. This integration aims to create a unified regulatory framework for both payment institutions and electronic money institutions, reducing the complexity that previously existed between these two sectors.

While this merger does streamline the regulatory framework, it may not necessarily lower barriers to entry. The requirements for an e-money license are expected to remain the same, if not become more stringent, which could limit the ease with which new players can enter the market. Previously, a Payment Institution (PI) license, and in some countries a Small Payment Institution, license, offered a more accessible entry point for smaller firms to establish themselves. However, the increased regulatory rigor could enhance banks' confidence in providing transactional banking services to licensed entities, as they benefit from stronger compliance measures.

Strengthened Regulatory Oversight

PSD3 introduces more stringent licensing and authorisation requirements for payment service providers. These include higher capital requirements[4], mandatory winding-up plans[5], and a more streamlined authorisation process[6]. The aim here is to enhance the stability and reliability of payment services across the EU. While these changes are designed to increase consumer trust and market integrity, they also pose significant challenges for smaller Fintech firms. The increased compliance demands may strain resources, particularly for startups and smaller companies, potentially leading to market consolidation as these firms struggle to meet the new requirements[7].

Enhanced Open Banking and Open Finance

PSD3 also brings significant enhancements to the Open Banking framework, including clearer guidelines for improved user protection and confidence, and expanded access rights for third-party providers. These changes are intended to remove existing barriers and improve the functionality of open banking across the EU[8].

The new rules offer an opportunity to deliver more robust and competitive services. Improved standards (dedicated data access interface[9] for ASPSPs[10] etc.) and increased access rights will enable Fintechs to integrate more seamlessly with banks, enhancing their ability to innovate and provide better services to consumers. Conversely, firms must also invest in more reliable infrastructure to remain competitive.

Security and Consumer Protection

Strong Customer Authentication (SCA)

Regarding PSR and according to EY[11], "A significant change in the cybersecurity domain is the expansion of security requirements to encompass payment card schemes, payment gateways, and merchants.

The regulation also now covers third parties to whom technical, operational, and communication services have been outsourced. This mandates more parties in the payment chains to implement systems such as Strong Customer Authentication (SCA)[12] to bolster payment security." The new rules also introduce other rigorous fraud prevention mechanisms, including enhanced transaction monitoring[13] and stricter liability rules.

Anti-Fraud Measures

Alongside the strengthened SCA, PSR introduces several new anti-fraud measures aimed at safeguarding consumer transactions. Key among these is the mandatory IBAN-name matching for credit transfers, which helps verify that the payee's details match the intended recipient[14].

Additionally, the regulation promotes enhanced data-sharing protocols[15] among payment service providers to detect and prevent fraudulent activities more effectively. While these measures may increase operational complexity, they are essential for maintaining a secure and trustworthy service in the eyes of consumers and regulators alike.

Conclusion

Regulations streamlining, better consumer protection, more competitive market… These proposals are set to significantly reshape the landscape of digital payments. For Fintech companies, this evolution presents both challenges and opportunities: while increased market compliance demands may strain resources, especially for small players, the potential for innovation and improved security offers a pathway to greater trust and adoption in the market. Firms that adapt quickly and invest in strengthening their infrastructure and compliance frameworks will be well-positioned to thrive in this new era. PSD3 and PSR are not just regulatory updates, they bring the foundation for the next waves of innovation and growth in payment services.

1) Proposal for a Directive of the European Parliament and the Council on payment services and electronic money services in the Internal Market amending Directive 98/26/EC and repealing Directives 2015/2366/EU and 2009/110/EC https://lc.cx/RM49-w
2) Proposal for a Regulation of the European Parliament and of the Council on payment services in the internal market and amending Regulation (EU) No 1093/2010 https://lc.cx/q29DXL
3) See Recital 5 of PSD3: "Even though the issuance of electronic money is regulated under Directive 2009/110/EC of the European Parliament and of the Council,31 the use of electronic money to fund payment transactions is to a very large extent regulated by Directive (EU) 2015/2366. Consequently, the legal framework applicable to electronic money institutions and payment institutions, in particular with regard to the conduct of business rules, is already substantially aligned. (...) It is therefore appropriate that the authorisation and supervision regime applicable to electronic money institutions is further aligned with the regime applicable to payment institutions.
4) See Recital 25 of PSD3: "To cater for the risks posed by their activities, payment institutions need to hold enough initial capital combined with own funds. Taking into account the possibility for payment institutions to engage in the wide range of activities covered by this Directive it is appropriate to adjust the level of the initial capital attached to individual services to the nature and the risks attached to these services." services to the nature and the risks attached to these services.
5) See the Explanatory Memorandum pf PSD3, p.7, "Licensing and supervision of payment service providers": "The procedures for application for authorisation and control of shareholding are mostly unchanged from PSD2, with the exception of a new requirement for a winding-up plan to be submitted with an application, but made fully consistent for institutions providing payment services and electronic money services."
6) See Recital 18 of PSD3: "To ensure a level playing field and a harmonised process for the granting of an authorisation to undertakings applying for a payment institution license, it is appropriate to impose to competent authorities a time limit of 3 months for the authorisation process to be concluded, after the receipt of all the information required for the decision."
7) See articles 5 and 6 of PSD3.
8) See page 5 of PSD3: "There are four specific objectives of the initiative, corresponding to the identified problems: 1. Strengthen user protection and confidence in payments; 2. Improve the competitiveness of open banking services; 3. Improve enforcement and implementation in Member States; 4. Improve (direct or indirect) access to payment systems and bank accounts for non-bank PSPs."
9) See p.5 of PSD3: "requirement for account servicing PSPs (ASPSPs) to put in place a dedicated data access interface; "permissions dashboards" to allow users to manage their granted open banking access permissions;"
10) Account Servicing Payment Service Providers
11) Rudrani Djwalapersad (22 Feb 2024) "PSD3 and PSR: regulatory uniformization for enhanced protection" https://lc.cx/EDjpSv
12) See article 85 of the PSR.
13) See p.10 of the PSR, "Operational and security risks and authentication": "A new provision is added requiring PSPs to have transaction monitoring mechanisms in place to provide for the application of strong customer authentication and to improve the prevention and detection of fraudulent transactions."
14) See p.6 of the PSR: "Improvements to the application of SCA, (...) extension of IBAN verification to all credit transfers." See Recital 104 of PSR: "'Unique identifier' should be understood as referring to 'IBAN'"
15) See article 84 of the PSR: "Payment service providers shall alert their customers via all appropriate means and media when new forms of payment fraud emerge…"