CONSUMER CHOICE CENTER

R16 CONSULTATION COMMENTS

Response to consultation

The Consumer Choice Center is an independent, nonpartisan consumer advocacy group that champions the benefits of freedom of choice, innovation, and abundance in everyday life.

As an organization, we are alarmed by the Financial Action Task Force's proposed card exemption revisions in the Explanatory Memorandum and draft revisions to Recommendation 16 released on February, 26 2024. If adopted, the revisions would create a situation in which increasing compliance requirements through more stringent FATF standards would violate the FATF's commitment to a risk-based approach. In doing so, the additional rules undermine the FATF's goal of effectiveness and create more systemic risk and poorer outcomes for consumer safety, privacy, and financial inclusion.

Section 1 A, paragraphs 9-11 of the 2014 guidance document define the risk-based approach as a principle of proportionality: authorities, financial, and card processing institutions must ensure that measures are commensurate with the identified and quantified risks (threats, vulnerabilities, or consequences) involved. Crucially, paragraph 13 in Section 1 B establishes the risk-based approach as a requirement all FATF recommendations must abide by (further set out in Recommendation 1 and the Interpretive Note for Recommendation 1).

However, the FATF's own Memorandum on Recommendation 16 fails to justify the expansion of regulatory scope (Section B, paragraph 4) and the obligatory introduction of sensitive personal information (Section C) as proportionate responses to AML/CF. References to specific money laundering practices are scattered throughout the text – the note on "smurfing" on page 3, a typology of crimes on page 4, and citing the FATF's report on Illicit Financial Flows from Cyber-enabled Fraud on page 6. These references are anecdotal AML/CF practices or provide a general overview of the harms associated with money laundering. What they do not do is specific evidence that monitoring and recording domestic and cross-border cash withdrawal of every cash equivalent to both parts of the payment chain (originator and beneficiary account) will result in a proportional drop in money laundering and terrorist financing to warrant such intervention. Beyond this, there is no quantitative estimate of the harms that will supposedly be prevented by the options

presented in the Memorandum.

Neither are the benefits of the decision clear when financial institutions already demonstrate successful risk management through their private efforts. Recommendation 10, Section 2 part d) on customer due diligence and enhanced due diligence requires financial institutions to take measures when they suspect ML/TF, even in cases that would otherwise be exempted. In practice, systems such as the Payment Card Industry Data Security Standard (PCI-DSS) and SWIFT Consumer Security Programme (CSP) go beyond the FATF revised Recommendation, providing risk management via encryption and tokenization that thwart untrustworthy networks and sources. The introduction of the proposals would be unnecessary from a risk-based point of view.

At worst, the FATF proposals neglect to consider the risks they themselves pose to the finance industry and consumers. By requiring the disclosure and recording of personal information for processing transactions throughout the payment chain under a unified system of FATF rules, the options presented in the Memorandum expose the entire system to the same security, privacy, and financial exclusion risks worldwide.

Finance was the second-most impacted sector by data breaches in 2022, with financial institutions suffering 566 data breaches and 254 million leaked records. The threat mainly originated from ransomware, software that installs malicious programs on bank computers, uses protocols to extract financial data, and then encrypts the information to demand a ransom from the victim. Ransomware attacks have almost doubled over the last years, from 34% in 2021 to 64% in 2023.

These data breaches and hacks pose significant risks to consumers, leading to identity theft, phishing attacks, and the illicit sale and disclosure of this information on darknet markets for purchase. A number of recent data breaches affecting healthcare and telecommunications services have already begun appearing online, exposing data from hundreds of millions of accounts with significant personal data. To see this applied to financial institutions will only end up being more costly and harmful to consumers.

Adopting ISO 20021 or equivalent standards under section B, paragraph 6 may theoretically increase interconnectivity in the financial system via a standard and consistent format for data exchange. Nevertheless, the same features leave the standards more susceptible

to malware and ransomware by multiplying the possible entry points, errors, and inconsistencies for a breach. By contrast, PCI-DSS and SWIFT CSP minimize the use of data as the first line of protection against fraud to mitigate the risks posed by malware and ransomware.

Consumer privacy is, of course, the other side of the equation. A common norm would make data transmission more granular in financial messages (allowing for more regulatory data in the name of transparency). Unsurprisingly, every cross-border withdrawal under Section C of the Memorandum includes extremely sensitive information like the full name of the originator, address, country, and town name, and the date and place of birth of the originator and beneficiary. The downside is that it exposes more sensitive data with every cyber-attack, error, or fraudulent attempt. The threatening ramifications are not just personal but legal, as the Memorandum is not taking all reasonable measures for data minimization under Article 25 of the European Union's General Data Protection Regulation (providing for "data protection by design and default") and could effectively be non-GDPR compliant (a requirement for handling financial information in the EU). Recommending a standard of end-to-end encryption of the most vital and sensitive financial data, while reserving only the minimally required information for open reporting would significantly reduce the privacy risks affiliated with the data collection and reporting.

Lastly, the Memorandum's proposals threaten to erode financial inclusion. Part of the FATF's stated goal of effectiveness is to provide access to safe, convenient, and affordable services to consumers from disadvantaged groups (low-income, migrants, minorities, or rural persons). The latest World Bank data indicators from 2017 show that only 31.5% of adults own a bank account, and just 50.6% have ever withdrawn from a financial institution in low-income countries, compared to 72.4% and 67.7%, respectively, in upper middle-income states.

Despite introducing a de minimis threshold of 1000 EUR/USD and nominally linking financial inclusion to de-risking in sub-section h, the Memorandum's Section C additional information provisions raise the compliance costs for ATM operators and cash processors across the board, which will result in less access to financial services for vulnerable consumers worldwide. After all, some consumers are likely to have incomplete or missing financial information, exposing them to extreme situations in which working abroad and sending vital remittances home will become more challenging.

The CCC recommends the following changes

- Acknowledging the privacy, security, and financial exclusion risks involved and the lack of proven benefits, maintain the existing scope of the exemptions under Section B 4 of the Interpretive Note and remove the requirements for additional financial information from Section C. Any references to the "name and location of issuing and acquiring financial institutions" and "withdrawals and purchases of cash and cash equivalents" should be deleted from the final text.

- Considering the lack of evidence of identical risks to warrant "same effects, same treatment", delete "payment transparency" and revert to the previous language referring exclusively to "wire transfers".

- Recommend a standard for end-to-end encryption of vital and sensitive financial data in line with existing industry practices to better protect consumers, financial institutions, and all end users, while leaving only necessary financial information open for reporting.