World Council

16 February 2024

Submitted Electronically: https://www.bis.org/bcbs/commentupload.htm

Basel Committee on Banking Supervision
Bank for International Settlements
CH-4002 - Basel, Switzerland

Re: Digital Fraud and Banking: Supervisory and Financial Stability Implications

Dear Sir or Madam:

World Council of Credit Unions (World Council) appreciates the opportunity to comment on the Basel Committee on Banking Supervision's (Committee) discussion paper regarding Digital Fraud and Banking: Supervisory and Financial Stability Implications (discussion paper).[1] Credit unions are cooperative depository institutions and World Council is the leading trade association and development organization for the international credit union movement. Worldwide, there are over 82,000 credit unions in over 98 countries with USD 3.6 trillion in total assets serving over 400 million physical person members.[2] World Council fully supports the efforts of the Committee to assess the supervisory and financial stability implications of digital fraud and requests the Committee consider the below responses.

Q1. Do you agree with the features and categories of digital fraud? Are there additional financial stability and/or prudential transmission channels from digital fraud to the banking system?

World Council agrees with the features and categories of digital fraud. We appreciate the inclusion of vulnerabilities on both the consumer and banking side of financial transactions. However, an additional feature should be explained to cover the sources of exposure that are outside the chain of a financial transaction but indirectly impact the authentication security features established by financial institutions. Features should be added specifically in the "deception or falsification category" to explain this missing area of vulnerability.

The discussion paper explains that this category "relies on the inability of a bank or its customers to appropriately distinguish a fraudster from a legitimate counterparty."[3] This may be due to insufficient processes and IT security within the financial institution. However, it does not mention the other areas of exposure that are outside the financial institution's control during the authentication process. For example, muti-factor authentication to verify a consumer's identity may fail due to a fraudster breaching a consumer's email and phone to receive verification codes. While the other categories explain features such as phishing, malware, and other

[1] See, Discussion Paper, Digital Fraud and Banking: Supervisory and Financial Stability Implications; https://www.bis.org/bcbs/publ/d558.pdf
[2] World Council of Credit Unions, *2022 Statistical Report* (2023), *available at*: https://www.woccu.org/documents/2022_Statistical_Report_EN
[3] See, Discussion Paper, page 4. https://www.bis.org/bcbs/publ/d558.pdf

methods directly related to consumer account information, it is important to note that those scenarios also extend beyond sensitive information directly tied to the financial transaction. Theft of a consumer's electronic footprint not tied directly to banking is also a critical feature of technology challenges, specifically in the authentication phase of a financial transaction that should be included.

Q3 Are there any additional, banking-specific, initiatives on digital fraud that could be pursued by the Committee?

World Council urges the Committee to explore the methods and ramifications in which the most vulnerable populations are targeted. Digital fraud is another challenge credit unions face in their mission for financial inclusion. While all consumers are at risk of digital fraud, often vulnerable populations are disproportionately impacted. For example, the elderly who may be more exposed to the technical expertise of fraudsters or immigrant communities unfamiliar with a different country's financial practices or language. The Committee provided helpful data related to different countries' financial transaction behaviors and risks relative to asset size. However, it would be helpful to learn from the Committee's understanding of digital fraud methods targeting vulnerable populations and the impact on supervisory actions.

WOCCU also requests the Committee consider additional education initiatives related to fraud activity and resources. The discussion paper notes that digital fraud clearly has an international element with cross-border implications. Large international banks will often have faster information related to new and developing fraud schemes and tactics due to their size and large reach of daily transactions. Credit unions serve their local community but understand many instances of fraud may originate outside of their borders. Additional resources from both international and national authorities would be beneficial as credit unions continue to adjust their security methods and their internal risk evaluations. Credit unions continue to focus on educating members about the types of fraud and prevention methods as well as improve their own security measures but additional resources from international standard setters with a global perspective would better support those activities.

World Council appreciates the Committee's continued focus on digital fraud and its impact on the stability of financial markets as well as on individual consumers. If you have any questions about our comments, please feel free to contact me at erinohern@woccu.org.

Sincerely,

Erin O'Hern

Erin O'Hern
International Advocacy and Regulatory Counsel
World Council of Credit Unions

World Council of Credit Unions, Inc.
99 M Street SE, Ste 300, Washington, DC 20003 • +1-202-638-0205 • +1-202-638-3410
www.woccu.org