March 11, 2024

Iowa Division of Credit Unions Regulatory Advisory Bulletin

Notification Requirements Following Data Breach:

Cyber and Data Security Breaches are increasingly areas of attention for the Division of Credit Unions. Iowa Code requires each Iowa state-chartered credit union to maintain an information security response program consistent with Title 12 of the Code of Federal Regulations, Part 748. Iowa Code Section 533.331. The response program is required to include procedures for notifying the Division of Credit Unions "as soon as possible after the credit union becomes aware of an incident involving unauthorized access to or use of sensitive member information that would permit access to the member's account." Iowa Code Section 533.331. Federal law also requires Iowa state-chartered credit unions to notify the applicable NCUA Regional Director and Iowa Superintendent of Credit Unions as soon as possible and no later than 72 hours after the credit union reasonably believes that it experienced a reportable cyber incident. See Appendix B to 12 C.F.R. Part 748. This notification requirement is equally applicable when a credit union's vendor, CUSO, or affiliated/non-affiliated third party's cyber or data security breach impacts the credit union or includes members' data.[1]

Neither Iowa law nor Appendix B dictate the manner in which a credit union should notify the Division of Credit Unions of a data breach. This Regulatory Advisory Bulletin expressly lays out the expectations and requirements of the Division of Credit Unions.

Requirements: As soon as possible and no later than 72 hours upon discovery of an incident involving unauthorized access to or use of sensitive member information, the Iowa state-chartered credit union is obligated to email the Iowa Division of Credit Unions at this address: Idcu_support@iowa.gov and the Director of Examinations (Kevin Gorman) at this address: Kevin.Gorman@iowa.gov. The subject line must include: "IMPORTANT Data Breach Notice." **The initial notification email to the Division should be limited in scope and contain NO sensitive information, unless this email is encrypted, password protected, or sent using secure mail.** The Division will confirm receipt of the credit union's notification as soon as practicable. Thereafter, the Division will reach out directly to the credit union regarding any additional information requests.

This Regulatory Advisory Bulletin is not intended to address any legal requirements or obligations related to a Cyber or Data Security Breach other than the notification requirements set forth in Iowa Code Section 533.331. Each Iowa-chartered credit union is responsible for understanding and following the additional obligations set forth in state and federal laws regarding Cyber and Data Security Breaches.

Katie Averill
Superintendent of Credit Unions
KA/dr

[1] This Regulatory Advisory Bulletin only articulates notification requirements under Iowa law and does not analyze any legal liability under Iowa State or Federal law.