*Setting a **Higher Level of Excellence** in Information Security & Compliance Services.*

Customer Security Awareness Training | by Mike Smith, AWS-CCP

It's not only a moral obligation for an institution to advise its account holders on protection of their identity and assets; it is absolutely recommended by myriad experts, sources, and FFIEC guidelines which state that financial institutions should have a policy within the Information Security Program to govern "Customer Awareness" (*FFIEC Information Security Booklet, II.C.16(a)*). Financial institutions should comply with that policy, providing some type of ongoing training to their customers, members, and consumers.

This training may be provided any number of ways: pamphlets, statement stuffers, and so on. More frequently, training is being delivered electronically as content on institutions' marketing websites, with reminders being dripped by email, text, e-banking logon banners, or printed on statements.

Other avenues include social media or updating the phone system on-hold recording to include comments about safeguarding personal information, as well as offering access to memberships in third party programs – remember to perform proper vendor reviews and risk assessments before offering these programs.

Divide the security awareness training into sections focusing on the audience, separating retail and commercial account holders. Scams, both off- and on-line, can be, and usually are, different for retail and businesses or nonprofits.

For high-risk and commercial account holder edification, ensure that institution policy and procedures are documented in agreements for services such as ACH, wire transfers, remote deposit capture (RDC), and other high-risk cash management transactions. Depending on size and complexity of the institution and the account holder, recommend or require that commercial account holders perform their own risk assessments and audits to ensure they are compliant with the institution's security controls and policies. Require or offer to review these assessments as part of regular reviews, such as RDC audits.

Explain the protections afforded within the institution's online solution, and how they apply to Federal Reserve Regulation E (https://www.federalreserve.gov/supervisionreg/regecg.htm) and electronic fund transfer.

Also include an explanation of how the institution might contact the account holder regarding their accounts and how the institution and employees will identify themselves. Keep it basic: "We won't ask you for your account number or password over the phone, or by email. And, make a direct line of contact available to the institution should the customer believe their accounts have been compromised.

Provide a list of required or optional security controls available to the account holder as they relate to the institution's systems. Include authorization controls, such as multi-factor authentication. Most importantly, ensure the statements and advice given are in line with the institution's Information Security Program and Electronic Banking policies, and coincide with training and resources given to institution staff.

If you have more questions, please contact 10-D Security for assistance with implementing a solid Customer Security Awareness program.