The Future of Two-Factor Authentication

I read with interest the article describing the new NYS Department of Financial Services (DFS) and the required regulations to commence in the next very few years (Al Alper, "What CPAs Need to Know about New York's New Cybersecurity Requirements," June 2017, http://bit.ly/2tr3CT7). We should congratulate the author on a timely and relevant topic. One important lede that was buried in the article is a required "two-factor authentication," which the proposed DFS rule included, and which despite much commentary (including that from the Technology Assurance committee and the NYSSCPA) survived the comment period.

I suspect that this will resemble the requirement by HIPAA for antivirus software; when that requirement was introduced, it was viewed as innovative, cutting edge, and expensive. Today, antivirus software is viewed as a required minimum for IT security, but by no means a fail-safe for cybersecurity breaches. From our collective experience, we should be careful not to fall into a false sense of security that somehow the upcoming DFS rules are the magic bullet needed to address cybersecurity threats.

Instead, CPAs (as advisors, and even as auditors) should recommend a solid risk assessment for IT, training, and risk management response that is risk-based, not just regulatory-driven. Of course, the new DFS regulations can be an impetus for creating such a discourse with prospective and current clients.

Yigal M. Rechtman, CPA, CFE, CITP, CISM
Fort Lee, N.J.

The Author Responds

I agree with Mr. Rechtman that, on the surface, two-factor authentication (2FA) trends like the much-vaunted antivirus software of the '90s and 2000s. I feel, however, that 2FA will enjoy greater staying power and a more lasting success because it creates a significant barrier to entry for hackers.

Unlike traditional anti-malware and even the latest anti-ransomware, 2FA relies on three layers of protection: a traditional login to the system, a secondary system that generates a randomized, single-use code, and human interaction to read and transcribe the code. This layered approach across disparate systems creates a substantial and significant barrier to entry for hackers, much more so than the traditional end point–based anti-malware program.

All of that said, Mr. Rechtman is correct that no system is foolproof; eventually, cybercriminals will find their way around