Snowballs and Biometrics

by [Steve Brown](#) Topics: [biometrics](#), [authentication](#), [cyber security](#)

Sometimes things show up unexpectedly. This happened in Siberia in the end of Oct. Along the beach off the Gulf of Ob in Northern Russia, giant snowballs were washing up. They stretched across 11 miles, and ranged in size from as small as a tennis ball to as large as 3 feet across. The press secretary for the Arctic and Antarctic Research Institute calls this a "primary natural phenomenon" with sludge ice, the effects of wind and temperature, and the position on the coastline. Sometimes it takes a natural phenomenon to remind us of the amazing things going on in the world. While not as cool as a giant snowball perhaps, the rise of biometrics in banking is amazing in its own right.

To quickly remind everyone, single factor authentication consists of something you know like a username and a password (or security code). Meanwhile, two factor authentication is based on something you know (like a password/security code) and something you have (like an ATM card or token). Finally, multi factor authentication builds on both of those by incorporating something you know (like a password/security code) with something you have (like an ATM card or token) and something you are (like biometrics including fingerprint, voice, etc.) or even a location (like geo location).

For their part, regulators have long required stronger authentication practices, but they haven't defined precisely how banks should accomplish this. Rather, banks are expected to use robust authentication methods appropriate to the level of risk. However, as technology shifts and crooks continue to press harder, banks are struggling with which authentication methods to choose and how many layers of protection to have. This has become a particular concern when it comes to mobile and online banking activities.

Some banks still rely on passwords alone for account entry, which can be problematic given how insecure passwords can be. Consider that in 2015, words like football, baseball and welcome ranked high on SplashData's top 25 "Worst Passwords" list. Perpetual favorites like 123456 and password ranked at the top. Moreover, according to a 2015 Telesign study, 73% of online accounts use duplicated passwords. As if that weren't bad enough, consider almost half of consumers (47%) rely on a password that hasn't been changed for 5Ys.

To get around the issue of passwords, some banks have taken the approach of requiring a passphrase, which is considered easier to remember than a password and more secure. Still other banks have gone to unique, 1x codes to complete a sign-on.

Still other banks have introduced biometric methods, like retinal scans, facial recognition, voice recognition or fingerprints. Certainly, fingerprint technology has gained traction in the past several years as phones have advanced. Deloitte even predicts there will be 1B smartphones with fingerprint readers in use by the end of next year.

But even fingerprints can be spoofed. Just recently, Kaspersky Lab warned that crooks are already selling skimming devices that they claim can steal fingerprints. This is troubling news for banks that

rely exclusively on fingerprints and is likely to gather more regulatory attention here in the US.

As you are trying to determine the best ways to secure your customers' accounts and your own data, remember that security is never completely foolproof. However, multi-layered authentication, encryption and other security methods can add additional levels of protection. After all, no one wants to be standing there with a tennis ball sized snowball in a fight with an aggressor using a 3 foot sized variety.

BANK NEWS

More Buyers

Research by Bank Director (surveyed bank executives and directors) around the M&A plans of banks finds that by the end of 2017: about 46% said they were likely or very likely to purchase another bank, but 76% of those asked said they were not considering selling their bank. Looks like interested buyers once again significantly outnumber interested sellers. Interestingly, by asset size even a whopping 72% of banks under $250mm (often cited as the most likely to sell due to economies of scale, profitability, etc.) said they did not plan to sell the bank vs. 28% who were open or interested in doing so.

US Growth

The Congressional Budget Office (CBO) projects an aging population and softness in productivity will keep GDP at 2.0% for the foreseeable future. Meanwhile the National Association for Business Economics (NABE) finds 80% of business economists' surveyed project GDP will be 2.5% or lower over the next 5Ys.

Board Presentations

Research by PwC of board members from financial services companies finds 57% wish board presentations were less formalized and involved more spontaneous discussion; 45% wish board discussions with management were less scripted or controlled; 60% wish board materials were somewhat shorter; 47% wish board materials contained less industry jargon and 45% wish board materials were analyzed to better remove outdated information.

Going Longer

FDIC data finds that over the past 10Ys long term assets with a maturity of 5Ys or more declined 13% at commercial banks with assets <$100mm, but jumped 74% at banks with assets $100mm to $1B.