Digital Destruction

cyber security encryption OCC

One of the benefits of the digital age is that it has become infinitely easier to be an information pack rat. A music library that once would have filled a bookcase with CDs now fits on your phone. Documents that would have once filled a garage can now easily be tucked away in the cloud. Keeping everything in digital form saves physical space, but it clutters cyberspace, and it also makes information vulnerable to cyber thieves.

The digital world is nothing if not inventive, so now there are programs to automatically delete files for you, including various types of messaging. At the same time, encryption methods are constantly being upgraded to make it harder for cyber thieves to break in.

If you're like most community banks today, you're probably dealing with both digital clutter and cybersecurity. But before you go too far down the auto-delete path or too deep into encryption mode, be aware that regulators have some thoughts here.

Bank examiners get really testy about certain things in the technology arena that include: the destruction of files or information related to banking that they might have wanted to examine and roadblocks to their ability to examine a bank's internal information. So it should come as no surprise that regulators have just issued a warning to banks about digital deletion and encryption processes that can that thwart examiners.

OCC Bulletin 2016-13 provides guidance to banks on retention of records and examiner access. In it, the OCC seems to also support innovation in the banking industry - up to a point at least.

"The OCC has become aware of communications technology recently made available to banks that could prevent or impede OCC access to bank records through certain data delete and encryption features," the bulletin states. "Use of communication technology in this manner is inconsistent with the OCC's expectations regarding data retention and availability."

If there's one situation you want to avoid as a bank, it's being inconsistent with any regulators expectations. The OCC goes on to give an example of the type of innovation that causes it to lose sleep: some chat and messaging platforms that promote an ability to "guarantee" the deletion of transmitted messages. As the OCC points out, permanently deleting internal communications, particularly if done in a relatively short time frame, conflict with OCC "expectations."

It may be a coincidence, but it is interesting that the OCC warning comes on the heels of the recent pitched battle between the government and Apple over the iPhone recovered in the investigation of the San Bernardino terrorist attack. The government wanted to know what was on that phone but couldn't crack the iPhone encryption, so it demanded that Apple reveal its secrets. Apple refused. After much court wrangling the

government finally broke into the phone on its own and backed off the case. That was in March and the OCC bulletin came out in April so it has us wondering. We also point out that some large banks have seen huge fines around such things as Libor fixing and other things, and the ability to delete messaging information automatically may be another reason. Who knows?

While the contents of internal community bank communications probably aren't matters of national security, they still represent information the government wants. The regulatory bulletin is a warning to banks that the government is similarly serious about its desire to have open access to digital information held by banks, and that it will not look kindly on methods that go too far to encrypt or auto delete that can block government access.