AMERICAN BANKER®

Put bank exam council in charge of data privacy

By Jeremiah Buckley | July 17, 2020

From the European Union to California and now other states and countries, data protection and privacy standards going into effect often share the same objectives, but have separate and different regulatory requirements.

This creates a confusing array of legal requirements that pose compliance and reputation risks for banks. It also deserves attention by the federal bank regulators that make up the Federal Financial Institutions Examination Council.

The rapid advance of artificial intelligence, the pervasive collection of data, and the demonstrated vulnerability of such data to theft by private parties and state actors has profound personal liberty implications.

As demand for digital has increased due to the coronavirus pandemic and stay-at-home orders, the public is more and more uneasy that few adequate data protections are in place. Conferring on consumers some control over their "digital persona" is an important emerging right that various state legislatures are seeking.

However, the problem for holders of data seeking to protect consumers is that the variation in requirements in multiple jurisdictions makes compliance maddeningly complex, expensive and subject to inadvertent violations. The internet is a borderless medium and does not lend itself to balkanized regulation.

But neither Congress nor the administration has articulated a way forward that would establish a uniform set of national rules, and neither seems likely to do so in the near future. Further, the Uniform Law Commission that promulgates model uniform state statutes appears to be a long away from producing a broader data protection/privacy law. And if it does, only then will the slow multiyear process of state-by-state adoption begin, assuming states are willing cooperate, which is by no means assured.

For the banking industry, fortunately there is a forum that can help cut this Gordian knot of multiple jurisdictional rules. The FFIEC has already ventured into this area, providing guidance regarding cyber risk management. But there are several other areas in which the FFIEC can take action.

First, it could set up an FFIEC Office of Data Protection charged with studying the spectrum of issues associated with data management by regulated institutions, including cyber risk and privacy law compliance.

Data is the lifeblood of the financial services industry. In chartering banks and credit unions, regulators are granting the right to handle the most sensitive customer data. It is clearly within the jurisdiction of these agencies to assure that the data that chartered institutions hold is treated with appropriate care and with proper regard for the interests of depositors, borrowers and other customers.

Among other things, this FFIEC data protection office could consider the practicality, costs and reputational risks associated with trying to comply with multiple privacy regimes established at the state level.

Second, the FFIEC can provide its own guidance regarding data protection/privacy for regulated entities. The FFIEC Information Security Booklet, which is part of its IT Handbook, already provides guidance to regulated institutions on the elements needed to establish a data security program. While continuing to enhance the Information Security Booklet in light of the changing threat environment, the FFIEC should also consider publishing a parallel data protection/privacy rights booklet.

Third, recognizing that the field of data protection/privacy rights is in the process of evolution, the FFIEC might consider convening a data protection advisory committee consisting of regulated financial institutions, privacy advocates and others involved in the public discourse on data protection, including a state bank supervisor and perhaps a state attorney general.

Whether or not a partial preemption of state laws for federally chartered or insured institutions is necessary is something that will emerge as the legislative and regulatory picture comes

into clearer focus. But it should not be taken off the table.

Some will say that any action the FFIEC takes in this area would be premature or unnecessary given that many state enactments provide an exemption for financial institutions for data covered by the privacy provisions of the Gramm-Leach-Bliley Act. But anyone who looks closely at the reality of most of these state law exemptions — including the one contained in the California law — will note that large swaths of data held and used by financial institutions (such as data used for marketing purposes) is not covered by these Gramm-Leach-Bliley exemptions.

Furthermore, federal financial regulators should be front-and-center looking out for the data rights of bank customers in a rapidly changing data analytic environment, not simply standing by as others define these rights.

Suddenly these issues, which have bubbled beneath the surface for some time, seem to be moving to the forefront. Now is the time to assert federal authority in an area of national policy that has important implications for individual liberty, as well as the country's economy and national security.

Data protection rules will impact competition, intentionally or inadvertently creating winners and losers based on data mobility and compliance costs. It is important for the federal financial regulators to develop a unified and rationalized stance on what is arguably one of the most important policy decisions confronting the financial services industry.

In coming to grips with these issues for the industry, the FFIEC may be able to supply a template for a broader set of standards that Congress could adopt for the economy as a whole.