Passwords And Customer Privacy

regulatory risk management

Summary: In banking, stringent privacy laws enacted in the US and abroad are forcing banks to question what they need to do to stay in compliance. We provide 3 key tips.

People typically use a few tricks to remember their passwords. Pew Research finds the most common ones are: memorize the password (86%), write it down (49%), save it in a note on a computer or mobile device (24%), save them in their internet browser (18%), or use a password management program (12%).

Passwords are one way to authenticate someone to maintain their privacy. In banking, stringent privacy laws that are being enacted in the US and abroad are starting to force banks to question what they need to do to prevent running afoul of regulators and law enforcement.

Indeed, since General Data Protection Regulation (GDPR) in the European Union (EU) became effective in May, this stringent privacy law, along with other tough ones passed in the US by various states, is adding pressure. Many banks have been asking themselves how these rules might impact them and the way they conduct business. These new regulations are already driving concerns about information-sharing among companies that deal with banks and operate within the industry.

Case in point: a year-long, previously undisclosed card transaction data-sharing arrangement between Mastercard and Google came to light in late August. It created controversy in the wake of the Facebook-Cambridge Analytica debacle earlier this year. The deal gave Google unprecedented insight into the online and offline spending habits of 2B MasterCard cardholders. It also raised tremendous consumer privacy concerns.

While most banks do not intentionally set out to access or share customer data in a way that oversteps privacy rules, the mere fact that you possess significant personal and financial information and interact with outside service providers may put your bank squarely in the midst of this data privacy conundrum. To help guide you, here are some things to consider:

Who and where your customers are. GDPR has typically been assumed to apply to companies that offer goods and services in the EU or have EU customers. Some of your business customers likely have activity overseas, so this could impact you too. Be very careful with EU citizens and US citizens who are living or working overseas. These cases should be reviewed with privacy lawyers to properly apply GDPR.

Stay informed and train. Regardless of your current geographic location, you should try to stay on top of the latest privacy rules. These rules are expanding and will likely affect you in some way, sooner or later. When that day comes, you will also want to be sure that you inform and train your staff of the new rules or changes in rules. Compliance personnel should work closely with other departments such as IT, marketing and sales, to be sure the proper procedures are updated and best practices continue to be used in all customer interactions.

Conduct a privacy assessment. Given the fact that the pendulum is swinging in the direction of greater data control and privacy for customers, bankers may want to proactively seek the advice of legal or regulatory experts. They could advise you on which rules and regulations could impact your customers' information to keep your bank secure in this changing area.

DEPOSIT OPPORTUNITY YIELDING 2.30%

In an effort to expand our relationships, PCBB is pleased to offer community banks a money market deposit account rate of 2.30%, subject to availability. Contact operations@pcbb.com.