

2017 SOCIAL MEDIA SURVEY

FINAL REPORT
MARCH 2018

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

The 2017 survey was designed as an outcome of RMA members' interest in ascertaining the range of practice regarding member institutions' respective social media policies.

The purpose of the survey was to capture the current status of social media policies across a range of RMA member institutions and to gather detailed information on current and best practices and challenges.

The final report provides participants' responses, while protecting the confidentiality of individual institutions by masking the source of the responses.

Note: Due to rounding, percentages in the tables may not add up to 100.

RMA staff contributing to the study were Edward J. DeMarco Jr., and Sylwia M. Czajkowska.

Institutions (14) that participated in the survey:

Anonymous
Amarillo National Bank
BB&T
First Bank
First Citizens Bank
First National Bank of Omaha
Frost Bank
Huntington Bank
Maine Community Bancorp
RBC
State Bank of Cross Plains
TCF Bank
TD Ameritrade
U.S. Bank

Disclaimer

The information contained herein is obtained from sources believed to be accurate and reliable. All representations contained herein are believed by RMA to be as accurate as the data and methodologies will allow. However, because of the possibilities of human and mechanical error, as well as unforeseen factors beyond RMA's control, the information herein is provided "as is" without warranty of any kind, and RMA makes no representations or warranties expressed or implied to a subscriber or any other person or entity as to the accuracy, timeliness, completeness, merchantability, or fitness for any particular purpose of any of the information contained herein. Furthermore, RMA disclaims any responsibility to update the information. Moreover, information is supplied without warranty on the understanding that any person who acts upon it or otherwise changes position in reliance thereon does so entirely at such person's own risk.

The report is provided to participating institutions for internal analytical and planning purposes only. As such, a participating institution may disclose the information to consultants and agents that are engaged to assist that participating institution in analysis and planning; however, such consultant or agent is prohibited from using the information for any purpose other than such analysis and planning for that participating institution.

About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, more than 18,000 of these individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in global financial centers.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk management principles, RMA keeps members informed and provides access to industry information at this site; publishes *The RMA Journal* and a variety of newsletters, books, and statistics; conducts workshops and seminars; holds conferences, including an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

Visit RMA at www.rmahq.org.

Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

EXECUTIVE SUMMARY

The survey was conducted by The Risk Management Association (RMA) between November 2017 and January 2018. Most of the questions were multiple choice with opportunities to provide comments. Some questions were open text, designed to provide information and insight about best and current practices.

A total of 14 responses were received from a wide range of financial institutions including community, regional, and large banks headquartered in the United States and Canada:

- Asset size below \$10 billion: 5 responses
- Asset size between \$10-50 billion: 4 responses.
- Asset size between \$50-100 billion: 0 responses.
- Asset size between \$100-250 billion: 2 responses.
- Asset size over \$250 billion: 3 responses.

In today's world, social media has become the new communication platform for many, including the banking industry. Social media is not only viewed for entertainment purposes, but also provides institutions with an opportunity to work. Easy access via laptops, tablets, phones and other gadgets is one of the reasons for rapid growth of social media usage. In order to make social media more useful and effective in the workplace institutions find it challenging to keep their employees familiar with social media policies.

When asked about having a formal, written social media policy, all of the respondents confirmed having such a policy in place. This is a change from the 2015 survey, when 90% responded positively to that question.

Response	2017	2015
Yes	100%	90%
No	0%	10%

According to the survey, 57% of the institutions allow their employees to use their personal social media accounts for business purposes. Among those whose social media policy allows for the use of personal accounts, half of the respondents implemented a software platform that curates content and reviews posts prior to publishing them.

Of those surveyed, 57.1% said that their company allows its employees to access social media through the organization's computer network. In the 2015 survey, participants indicated as well that their employees are allowed to access various social media channels for personal purposes on company-owned and issued hardware, such as computers, laptops, tablets, and smartphones.

Approximately 54% of survey respondents require that employees post a disclaimer on their personal social media profiles or within their social media posts indicating that the views included in their social media interactions do not necessarily represent those of their employer.

Making employees aware of their company’s existing social media policy seems to be more significant for institutions. With respect to reviewing their social media policy with employees, 86% of institutions review it at the time of hiring employees, about 79% make it an annual exercise, 79% have the policy posted on the intranet, and 57% pay attention to it when material changes are made.

Response	2017	2015
At the time of hiring	85.7%	67%
Annually	78.6%	40.9%
It’s posted on the intranet for review	78.6%	50%
When material changes are made	57.1%	44.3%
Other (please specify)	7.1%	

For almost 54% of responding institutions, social media is not used for fraud detection or general investigative purposes. Those who use it for fraud detection purposes shared a more detailed explanation of how this is being accomplished in their institutions. Out of those who answered “yes”, 40% indicated that the use of “ghost/shadow accounts” is permitted. The procedures on the proper use of social media in the fraud detection area are established and the outline is communicated in 80% of cases.

Insights

Please see the following pages for detailed responses and examples of the range of practices that banks employ for social media.

Thank you to RMA member banks for contributing to this benchmarking study. The full report is available to those institutions that contributed to the study.