



## TOMPKINS FINANCIAL CYBERSECURITY STATEMENT

Tompkins Financial Corporation employs an in-depth, layered, defensive approach that leverages people, processes and technology to manage and maintain cybersecurity controls. Tompkins employs a variety of preventative and detective tools to monitor, block, and provide alerts regarding suspicious activity, as well as to report on any suspected advanced persistent threats.

As a general business strategy we have a robust, comprehensive and detailed Information Security Policy and Information Security Strategy. We perform annual IT risk assessments and run an enterprise IT audit program. This framework allows Tompkins to identify gaps, document solutions and plan for cybersecurity improvements. In addition, one of the most important things we do to protect our systems and customer information is continuous process improvement of our policies, standards and practices to ensure we are dealing with emerging threats and practicing sound safeguarding techniques for our customers.

Some specific technologies and practices we deploy to protect customer information are:

- Layered security (many security technologies and controls distributed across various attack avenues)
- Firewalls
- Intrusion Detection Systems (IDS)
- Anti-virus & malware detection
- Vulnerability and penetration testing
- Data encryption
- Advanced fraud alerting and prevention tools
- 24 x 7 security alerting and monitoring

Questions may be directed to:

Leon J. Brockway Jr.  
Information Security Officer  
Tompkins Financial Corporation  
P.O. Box 460, Mail Stop 50, Ithaca, NY 14851  
(Office) 607-274-7684 ext. 19464  
(Cell) 443-745-8942