Auszug aus der Rahmenvereinbarung über die Teilnahme am Online-Banking / Telefon-Banking und am Elektronischen Postfach:

9 Sorgfaltspflichten des Teilnehmers und Schutz des Teilnehmersystems

Das für das Online-Banking vom Teilnehmer genutzte System ist durch technische Maßnahmen gegen das Ausspähen der Sicherheitsmerkmale zu sichern. Es ist ein Betriebssystem einzusetzen, das dessen Hersteller für den Zugang zum Internet vorgesehen hat und für das er bei Bedarf Programmänderungen (z. B. Sicherheitspatches) zur Verfügung stellt, die erkannte Sicherheitsrisiken beheben. Die Systemeinstellungen sind entsprechend den Herstellerempfehlungen vorzunehmen. Bietet der Hersteller mehrere Sicherheitsstufen an, ist eine hohe Sicherheitsstufe einzustellen. Zusätzlich ist – soweit technisch verfügbar – das System durch ein Antivirenprogramm zu schützen sowie der Datenverkehr durch ein Firewallprogramm zu kontrollieren. Betriebssystem, Programme, die den Zugang zum Internet vermitteln (z. B. Browser) sowie die installierten Schutzprogramme sind nach den Empfehlungen des jeweiligen Herstellers aktuell sicher zu halten. Weiterführende Hinweise zum Schutz des Teilnehmersystems können den Sicherheitshinweisen der Sparkasse entnommen werden, die auf den Internetseiten für das Online-Banking veröffentlicht und aktualisiert werden. Bei Nutzung der Chipkarte als Zahlungsinstrument hat der Teilnehmer nur den von der Sparkasse gesondert mitgeteilten Lesegerät-Typ zu verwenden. Beim smsTAN-Verfahren darf das Gerät, mit dem die TAN empfangen werden (z. B. Mobiltelefon), nicht für das Online-Banking genutzt werden.

Bei Nutzung des pushTAN-Verfahrens hat der Teilnehmer die S-pushTAN-App durch die Vergabe eines sicheren Passwortes zu schützen. Das Betriebssystem des mobilen Endgeräts darf nicht entgegen den Empfehlungen des Herstellers durch Jailbreak, Rooten oder ähnliche Eingriffe verändert werden. Zusätzliche Software, insbesondere Apps, dürfen nur aus sicheren Quellen geladen und installiert werden. Die Sparkasse ist berechtigt, das pushTAN-Verfahren zu sperren, wenn das pushTAN-Gerät nicht gemäß den Herstellerempfehlungen eingestellt ist und bleibt.