-----Original Message-----
From: DJenni7474@aol.com [mailto:DJenni7474@aol.com]
Sent: Thursday, August 17, 2000 1:18 PM
To: public.info@ots.treas.gov
Subject: Docket No. 2000-51

August 12, 2000

Manager, Dissemination Branch
Information Management and and Services Division
Office of Thrift Supervision

Dear Sir or Madam:

We appreciate this opportunity to comment on the proposed guidelines for

establishing
standards for safeguarding customer information. I represent a small
($145
million in
assets) community-oriented savings bank in Frankfort, Kentucky.

While we certainly believe that this is an important topic, we do not
see the
need for a
regulation of such guidelines and believe that is has the potential to
create
a significant
burden for small community banks. Security of its information has
always
been a
primary concern for banks, but the method to achieve this security will
vary
with the size
and complexity of the institution. As with many regulations, we fear
that
the guidelines
and examiner training will most likely reflect standardized measures
that
would be
expensive and unnecessary for smaller banks.

I will briefly discuss some specific areas for which we believe the
regulation, as
proposed, is excessive.

Mention is made of service bureaus and the transfer of data from the
bank to
service
bureau. Most small banks rely on such bureaus to handle a majority of
its
processing
function. Small banks also rely on the expertise of these bureaus in
protecting our

1

customer information.   Currently, the FFIEC examines our service bureau, as
does an
independent auditor, for a variety of issues including the security of the
information on
the system. We rely on these outside opinions and the expected compliance of
reputable
service bureaus, and do not see how further regulation or requirements for
our action
would lead to results that are more meaningful.

The language whereby we would implement controls to "grant access [to information]
only to authorized individuals" is of great concern. This is entirely impractical in a small
bank and could result in significant costs for remodeling storage facilities
or moving
information off-site (at which point it would very likely be less secure).
We believe in
safeguarding such information from the public or from information predators,
but we
must trust our employees to abide by the strict confidentiality requirements
already in
place.

We also believe that while crafting an information protection plan is not
particularly
burdensome, testing of the plan could be expensive and time consuming and
result in very
little meaningful information. If testing is required, exceptions should be
granted for
procedures that are self-evident (such as a locked vault) or which can be
tested through
the software of the service provider (such as access via passwords). The
discussion of
independent testers would be expensive and potentially dangerous in that we
would
potentially be divulging information regarding our security system to an

outside party and
their employees whose integrity is unknown to us.

We have not found that requiring background checks for new employees is necessary or
practical. A meaningful check is expensive and often lacking in results.

As mentioned, we do not believe a problem exists at our community bank and
frankly
have not heard of many such problems elsewhere. We will be taking the necessary steps
to comply with the new privacy act, although we believe we have complied with

2

the spirit
of the act during our entire existence. Part of privacy is the security
of
our customer's
information and again, an area of banking that we have always taken very

seriously.
Additional regulation would be a superfluous and probably expensive
undertaking.

Sincerely,

Don D. Jennings
Executive Vice President
First Federal Savings Bank
P.O. Box 535
Frankfort, KY 40602
(502) 223-1638