



SEP11'06 PM 1:02 BO

Information Technology Center ■ 24 McKinley Avenue ■ Endicott, NY 13760-5491 ■ (607) 754-7900 ■ FAX (607) 754-9772
Credit Union Center (607) 786-2000 ■ FAX (607) 786-5718

September 5, 2006

Ms. Mary Rupp
Secretary of the Board
NCUA
1775 Duke Street
Alexandria, VA 22314-3428

Re: Identity Theft Red Flags and Address Discrepancies Under the FACT ACT of 2003

Dear Ms. Rupp:

On behalf of Visions FCU of Endicott, New York, I would like to respond to your the proposed joint agency rulemaking concerning Identity Theft Red Flags and Address Discrepancies Under the FACT ACT of 2003.

We object to the need for this regulation and the additional recordkeeping burden it will cause financial institutions, without any notable benefit to the public.

There is no doubt that the crime generally referred to as "Identity Theft" is increasing in severity and occurrence in financial institutions throughout the country. Losses to Financial Institutions and their insurance carriers continue to increase from this sort of crime. The rulemaking proposes to regulate that Financial Institutions have a written program based upon a risk assessment that will:

- Identify Red Flags relevant to detecting Risk to customer/members or to the safety and soundness of the financial institution during the course of business or when opening an account;
Assess whether the Red Flags detect evidence of identity Theft
- Mitigate the risk of this Identity Theft
- Train Staff to implement the program
- Oversee service provider agreements

The problem is that most financial institutions, their service providers (including their card companies), and their insurance companies have already taken action to mitigate losses and the risk to their customers/members. For example, our insurance carrier, CUMIS, recently toughened the minimum card security requirements our card programs were required to have if we wished to keep the portfolio insured because of problems with card fraud. Our credit union receives faxes from a Fair Isaacs monitoring service almost immediately after an ATM or Debit card is used in a suspicious manner or with an overseas address to investigate. Like all credit card issuers, we receive warning reports on other suspicious usage. All staff members have received training on Phishing and Identity theft, and we have specifically trained personnel that work in our plastics, audit, and fraud departments.



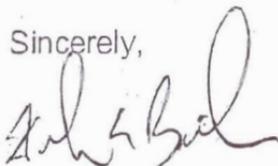
The fact is that losses that financial institutions, card issuers, and insurance companies have already incurred has already resulted in Identity Theft ID systems and policies being built into any modern day financial institution. No further regulation is needed to codify identification of red flags and discrepancies as described in this regulation. The regulation is superfluous and too late to help consumers or financial institutions.

What is needed is government action and international cooperation to stop and prosecute the national and international criminals behind many of the fraud and "Phishing Scams" we and our members suffer from –not another regulation telling us something we already know about and are acting on. I cannot remember the last time any "Phisher" that cost our credit union or insurance company money was shut down by the police or federal authorities.

Another way to protect the public would be through Government financed education for the public on how to protect their private information and not fall prey to the crooks that are out there trying to steal their information. Our credit union and many other financial institutions have undertaken doing this on our own.

We appreciate the opportunity to comment on the proposed rule changes.

Sincerely,

A handwritten signature in black ink, appearing to read "Frank E. Berrish", written over a light blue rectangular background.

Frank E. Berrish
President/ CEO