

FRAUD ALERT

Vishing Scam Targets Consumers

Consumers in many areas of the United States have been receiving automated “Vishing” telephone calls impersonating a local financial institution. The automated calls have gone out to thousands of residents regardless of which financial institution they patronize. It is clear that the perpetrators of this scam are not in possession of specific information for the financial institution that they are impersonating.

SCAM ARCHITECTURE

- 1. A consumer receives a pre-recorded call identifying a specific local financial institution. The message informs the consumer that his or her personal bank accounts have been frozen. The message advises the consumer to immediately input their ATM or debit card number, expiration date, and PIN to reactivate the affected accounts. The CV2 digits from the back of the card may also be requested.**
- 2. Calls appear to be made from various telephone numbers. The automated phone calls are most likely being made from a Voice over Internet Protocol (VOIP) telephone service using various telephone numbers that are attributed to this scam.**
- 3. Unauthorized ATM withdrawals are occurring immediately in Spain (and possibly other countries) as this scam develops.**

Please contact your local Police Department if you become aware of any such scam.