1.) A simple way to bypass the restriction would be to use a VPN to trick the website into thinking the request came from an actual Californian user. With a VPN, your request is sent to a third-party server, in this case, one in California, which then makes the request to the website on your behalf. Since the server is in California, its IP address is a Californian one, so the request is accepted and thus you can gain access to the website outside of California.

2.) The bank would not be able to use the old SSL certificate, as individual SSL certificates are either tied to a single domain, or tied to multiple subdomains of a single domain.

3.) The benefit is that public-key authentication uses a computer to generate the key, while password authentication relies on a human to create the password. Some people are lazy and use super insecure passwords like "password", but a computer will always generate the keys randomly, so there is no chance of a key being easy to guess or crack.

4.) Using many rounds for a password hashing algorithm ensures that any user who wishes to build large a table of hashes, say for a brute force attack, requires far more computing power than if the passwords were hashed using fewer rounds.

5.) An attacker can poison a DNS cache by inserting malicious entries. When the DNS server fetches this entry from the cache, then the user, rather than being sent to their intended destination, they are sent to the IP address stated in the cache, which may be the address of a malicious site.

6.) DNS amplification is a form of DDoS attack where the attacker sends a malicious request to an open DNS server that overloads the victim with a very large response from the DNS server. This response sends large amounts of traffic to the victim which may slow down or disable their systems, thus it is a DDoS attack.

Source: `https://www.cisa.gov/news-events /alerts/2013/03/29/dns-amplification-attacks`