

Jury Duty Scam (posted 7/30/07)

Consumers are advised to be on alert for a new identity theft exploit known as the "Jury Duty Scam". In this scam, the fraudster telephones their victim posing as a local court official who claims the victim has failed to report for jury duty, and as a result, a warrant has been issued for their arrest. The victim will rightly claim they never received any jury duty notifications. To "clear things up", the fraudster then asks for confidential information (i.e., social security number, birth date) for "verification" purposes or payment information (i.e., credit card number, bank account details) for alleged fines.

Consumers are urged not to give any personal information over the phone! These fraudsters are attempting to commit identity theft by appealing to the victim's sense of social conscience and fear of prosecution. VISA, the Federal Bureau of Investigation (FBI) and Snopes.com all advise consumers to never give out confidential or personal information when receiving unsolicited phone calls or e-mails. Additionally, court personnel will never ask for private information over the phone and typically only communicate via traditional mail.

Loss Prevention Recommendations

- Always verify the legitimacy of the caller by asking for official company or agency contact information, and then using directory assistance to verify and cross-reference the information given.
- Never solely rely on the phone number the caller provides as a means of verifying the authenticity of the call. Scam artists will often have an accomplice answer the phone to appear legitimate in the event of a return call.
- For e-mails, never respond directly to or click on a link in the e-mail. Always close the e-mail and open a new Web browser window to go to the official company or agency website to verify the authenticity of the e-mail.
- No matter how official the caller sounds or the e-mail appears, legitimate businesses or government agencies will not ask for sensitive, personal or financial information in their correspondence. This should always be a red flag.

Please also see our Loss Prevention Recommendations in the Scam Alerts page of our website.