



INTERNET CRIME COMPLAINT CENTER'S (IC3) SCAM ALERTS



This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

NEW TWIST ON EXTORTION/HIT MAN SCAM

The IC3 has received several complaints referencing a new twist on the [extortion/hit man scam](#), which is now targeting nannies and day care providers. The fraudster contacts the potential victims via email claiming their team was hired by a friend of the victim to "terminate" them. The fraudster demands amounts ranging from \$150,000 to \$250,000 to call off the hit and claims he will hand over a tape containing evidence as to who hired him once the amount is paid. The recipient is threatened with murder and the kidnapping of the children in their care if they fail to comply.

The majority of the victims had some affiliation with a nanny position and speculated that the fraudster must have obtained their contact information through an online classified ad offering their services as nannies. Others stated they had advertised online that they were seeking a nanny, while one victim was reportedly a day care worker.

PAYMENT PROCESSOR POSSIBLY CONDUCTING A PONZI SCHEME

Since January 2010, the IC3 has received hundreds of complaints regarding a website that victims reportedly used to transfer money for the sales of firearms; however, the website has not allowed them to withdraw the funds after their merchandise was sold.

The website claims to be a payment processor to be used as an alternative to other familiar online payment transfer services and was created to allow for the purchase of items that others of its kind do not allow (e.g., firearms). The website encourages consumers to use their services by advertising that they send money to consumers or anyone with an email address, an individual can easily pay for anything using the web, and sign-up is free, quick, and easy.

The website appears to have been set up as a legitimate business but shortly after operations began, customers started experiencing funding delays. Ultimately, customers who received funds only received partial payments, and those payments were delayed by months.

Additional research indicates that the money submitted for transfer may have been fraudulently misappropriated. This scam appears to have become a Ponzi scheme with previous customers being paid by funds from new customers.

FRAUDSTERS PREYING ON INDIVIDUALS WHO ARE WANTING TO ADOPT

The IC3 received information from law enforcement and complaints filed with the IC3 concerning an adoption scam. The scam is an attempt to collect personal information and funds from individuals seeking to adopt a child. Victims reported responding to on-line advertisements for adoptions, such as "Baby Needs A Home." The operators of the site are fraudsters who claimed to have an overseas orphaned child in need of adoption. Preying on victims' emotions, the fraudsters explained how they promised to care for the child after the mother's death.

The fraudsters said they were not affiliated with an adoption agency because no such agencies exist in their area. Nevertheless, they asked the victims to send pictures of their family and to complete forms that required personal information such as Social Security Number and their mother's maiden name. Fraudsters sent the victims a birth certificate and

pictures of a child. One victim reported that the birth certificate appeared altered. Fraudsters told victims to send hundreds of dollars via money order, credit card, or wire transfer to a bank account for legal fees. The fraudsters claimed they would "ship" the child upon receipt of the funds. Instead, the fraudsters pocketed the money gained from the scam and provided no children for adoption.

For more information regarding online scams visit our [Press Room](#) page for the most current Public Service Announcements.

<https://www.ic3.gov/media/default.aspx>