County of Santa Clara
Office of the District Attorney

August 21, 2014

FRAUD ALERT

THE EMAIL BELOW IS A COMPLETE FAKE/ FRAUD!!!!

From: Amazon.com [mailto:amazon@financial-department-invoice.com]
Sent: Tuesday, August 19, 2014 12:28 PM
To: ____
Subject: Order #2668612995699 [Status: Payment Pending]

Dear _____,

We would like to inform you that Amazon doesn't offer telephone support at present. As an online company, we focus on providing the best possible support to our community through email. This ensures our communication is consistent, and enables us to keep a precise record of all communication between us and our members. We will be able to assist you 24/24 h via email. Amazon wants to ensure that everyone who participates in the Amazon community has a safe and enjoyable experience. These rules apply to buyers, sellers, participants on the community boards and even Amazon employees.

We assure you that this transaction is covered under protection of Amazon FPS. Transactions with this seller are covered by purchase protection against fraud and description errors. You should locate and find the closest MoneyPak Store Locator to your home address and go there with cash. For security reasons the Green Dot-MoneyPak needs to be completed in person at any CVS/Pharmacy, Dollar General, Kmart, Family Dollar, Rite Aid, 7-ELEVEN, and anywhere you see the Green Dot-MoneyPak sign. Go with cash, No Online or Credit Card and pick up a Green Dot-MoneyPak from the Prepaid Product Section or Green Dot display and take it to the register. The cashier will collect your cash and load it onto the Green Dot-MoneyPak. After you purchased the MoneyPaks please reply us the MoneyPak Numbers (14 Digits Number off the back of your MoneyPaks) and send the scanned copy of your payment receipts by fax or email and a scanned copy off the back of your Moneypaks, where we can see the MoneyPak Numbers, so we can add them to the files and validate your payment.

If there is anything else you need to know, don't hesitate to contact us. Please reply to this email by keeping the subject line unmodified in order for your case to be recognized and your question answered in an instant.

Your funds will not be released to the Seller until you have received and approved the vehicle you are purchasing.

Sincerely,
Amazon FPS Customer Support
Vehicle Purchase Protection Program

The above email looks like it comes from Amazon- it doesn't. Here's what Amazon has to say about it:

1. Check the website address

Genuine Amazon Payments websites are always hosted on one of the following domains:

- https://payments.amazon.com/
- https://resolutioncenter.payments.amazon.com/
- https://authorize.payments.amazon.com

Sometimes the link included in spoofed e-mails looks like a genuine Amazon Payments address. You can check where it actually points to by hovering your mouse over the link--the actual website where it points to will be shown in the status bar at the bottom of your browser window or as a pop-up.

We *never* use a web address hosted on a domain other than the ones listed above. For instance, variant domains such as " http://security-payments-amazon.com/. . ." or an IP address (string of numbers) followed by directories such as " http://123.456.789.123/payments.amazon.com/. . ." are not valid Amazon Payments websites.

Alternately, sometimes the spoofed e-mail is set up such that if you click anywhere on the text you are taken to the fraudulent website. Amazon.com will never send an e-mail that does this. If you accidentally click on such an e-mail and go to a spoofed website, do not enter any information; instead, just close that browser window.