December 20, 2022

*****CONSUMER ALERT*****

ATTORNEY GENERAL RAOUL URGES ILLINOISANS TO WATCH OUT FOR GRINCHES, SCROOGES AND ONLINE SCAMMERS

Chicago — With only a few days left in the holiday shopping season, Attorney General Kwame Raoul is reminding Illinoisans to take precautions when shopping for or selling items online. Raoul is warning that scammers may use fake websites, fake mobile apps and fake social media advertisements to trick consumers into giving up their personal information and paying for products that will either never be delivered or cost more than they are worth.

"As the holidays draw near, it is important to be on the lookout for signs of fraud, as scammers are waiting to prey on consumers finishing up their holiday shopping," Raoul said. "This year alone, my office has received approximately 1,200 complaints from consumers relating to online purchases. By taking just a few precautions, consumers can educate themselves and quickly identify potential fraudulent transactions before they occur, saving money and headaches this holiday season."

In particular, Raoul is reminding buyers to be careful when using peer-to-peer ("P2P") payment methods, like Zelle, PayPal, Venmo and Cash App, with people they don't know, since P2P transactions do not offer the same level of protection as traditional credit cards.

Attorney General Raoul is offering the following tips to consumers to shop smart, sell smart and avoid scammers this holiday season:

- **Avoid fake websites.** Fraudulent websites may look like the real thing and may even have a similar website address. Double-check that you have typed in the right website address and check that phone numbers and addresses listed on the website are genuine in case you have questions or problems.
- **Read reviews of online businesses prior to purchase if you are shopping with a website you haven't used before.** Sites such as the Better Business Bureau may show any recent complaints against a particular business. More focused information can also be found by doing an online search of a company or seller's name along with the words "scam" or "review."
- **Be careful clicking links that were sent to your email or phone from suspicious or unfamiliar e-mail addresses.** Never give a third-party remote access to your computer or download a company's software just to make a purchase. These may be "phishing" or "smishing" scams to trick you into going to a fake website or installing a virus on your device.
- **Never give out private information – such as your social security number, payment information, usernames or passwords in an email or a pop-up "help" or chat box.**
- **Remember that just because a website is at the top of the search results doesn't mean it's the official website.** Scammers may use ads and sponsored links to trick you into going to their websites.
- **Be knowledgeable about Drop-Shippers.** Drop-Shippers don't own their inventory and only act as middle-man between you and a manufacturer. Dishonest Drop-Shippers may try to trick you into believing they are the manufacturer, charge you extra fees, or deliver you counterfeit goods or poor quality goods – if they deliver anything at all. Along with researching the legitimacy of a website, be sure to make a record of your transaction (for example, take a screenshot of your order receipt and order number) to help you with a later dispute.

- **Pay for online purchases with a credit card.** Transactions paid with a credit card are protected by the Fair Credit Billing Act, generally limiting your liability for fraudulent charges. Paying by debit card, prepaid cards, gift cards and cash do not offer the same safeguards. No matter what payment you use, make sure you're paying attention to high interest rates, calendaring payment dates, and sticking to a budget to stay out of debt.
- **Be wary if an online retailer or website does not accept credit card payments and requires that you pay by wire transfer, money order, gift card or cryptocurrency.**
- **Be careful when using P2P transactions.** Ensure you double check the recipient's information like name, phone number, email address or profile photo before hitting the send/confirmation button, and avoid sending or receiving money from anyone you don't know or trust. If you are sending money to someone for the first time, have them send you a "request" before you send the money or send them a small test amount – as little as one dollar – to make sure you're not sending money to the wrong person who just has a similar name.
- **Use multifactor authentication or two-step verification on P2P apps to make it harder for scammers to take over your account.**
- **Read the fine print to make sure there aren't hidden costs or obligations that could sign you up for recurring charges, like a monthly or annual subscription.**
- **Ensure you receive a delivery date.** If a seller doesn't promise a ship time in their ad, they must ship your order within 30 days of receiving your name, address and payment, unless they explain delays and give you the option to cancel and receive a refund.
- **Check a website's privacy policy to find out information being collected about you and how the website will use that information.**
- **Price-check items on different sites to help determine if a deal is too good to be true, or conduct a reverse image search of the item to see the true manufacturer and the original price.**
- **Sign up for free fraud alerts from your bank or credit card.**
- **Use different usernames and passwords for all your accounts, keeping the password in a secure place and changing the password every 6 months.**

If you think you have been a victim of a scam, you can file a complaint with the on the Attorney General's website or by calling the Attorney General's Consumer Fraud Hotlines:

1-800-386-5438 (Chicago)
1-800-243-0618 (Springfield)
1-800-243-0607 (Carbondale)

1-866-310-8398 (Spanish-language hotline)