ONLINE SCAMMERS REQUIRE PAYMENT VIA MUSIC APPLICATION GIFT CARDS

Complaints filed with Internet Crime Complaint Center (IC3) from 2017 show online scammers are asking victims to pay fraudulent fees using music application gift cards as part of multiple fraud schemes. These schemes include auction frauds, employment/opportunity scams, grandparent scams, loan frauds, romance scams, ransomware, tax frauds, and various other online schemes.

In this scam involving music application gift cards, the perpetrator directs the victim to a specific retailer to obtain music application gift cards of varying amounts. Once the victim has purchased the gift cards, the perpetrator directs the victim to reveal the numbers on the back of the cards and provide them to the perpetrator via telephone, email, text, or a designated website. Once the perpetrator obtains the music application gift card data, the perpetrator either continues to request additional funds through more gift card purchases or ceases all communication with the victim.

The financial impact to victims can range from hundreds to thousands of dollars. IC3 victim complaint data from January through June 2017 involving music application gift cards indicate that these scams have impacted hundreds of victims with reported losses exceeding $6 million.

This scam is also associated with other fraud scams involving victims having won a prize, needing to pay a tax debt, having qualified for a loan, or that a friend or relative is in trouble and needs a payment via music application or other prepaid gift card to assist.

GENERAL ONLINE PROTECTION TIPS

- Recognize the attempt to perpetrate a scam and cease all communication with the perpetrator.
- Research the subject's contact information online (e.g., email address, phone number); other individuals have likely posted about the scam online.
- Resist the pressure to act quickly. The perpetrator creates a sense of urgency to produce fear and lure the victim into immediate action.
- Never give unknown or unverified persons any personally identifiable information (PII).
- Ensure all computer antivirus and security software and malware protection are up to date.
- If you receive a pop-up or locked screen, shut down the affected device immediately.
- Should a perpetrator gain access to a device or an account, take precautions to protect your identity. Immediately contact your financial institution(s) to place protection on your account(s), and monitor your account(s) and personal information for suspicious activity.
- Always use antivirus software and a firewall. It is important to obtain and use antivirus software and firewalls from reputable companies. It is also important to maintain both of these through automatic update settings.
- Enable pop-up blockers. Pop-ups are regularly used by perpetrators of online scams to spread malicious software. To avoid accidental clicks on or within the pop-up, it is best to try to prevent them in the first place.
- Be skeptical. Do not click on any emails or attachments you do not recognize, and avoid suspicious websites.
- If you receive a pop-up or message alerting you to an infection, immediately disconnect from the Internet to avoid any additional infections or data loss. Alert your local FBI field office and file a complaint at www.ic3.gov.

FILING A COMPLAINT

Individuals who believe they may be a victim of an online scam (regardless of dollar amount) can file a complaint with the IC3 at www.ic3.gov.

In reporting online scams, be as descriptive as possible in the complaint by including:

- Name of the subject and company.
- Email addresses and phone numbers used by the subject.
- Web sites used by the subject company.
- Account names and numbers, and financial institutions that received any funds (e.g., wire transfers, prepaid card payments).
- Description of interaction with the subject.

Complainants are also encouraged to keep original documentation, emails, faxes, and logs of all communications. To view previously released PSAs and scam alerts, visit the IC3 Press Room at www.ic3.gov/media/default.aspx.