APPENDIX A: Glossary of Scam Type Definitions

ADVANCE FEE LOAN	In this scam, a loan is guaranteed, but once the victim pays up-front charges such as taxes or a "processing fee," the loan never materializes.
BUSINESS EMAIL COMPROMISE	This financial fraud targets businesses engaged in international commerce. Scammers gain access to company email and trick employees into sending money to a "supplier" or "business partner" overseas.
CHARITY	Charity scams use deception to get money from individuals who believe they are making donations to legitimate charities. This is particularly common in the wake of a natural disaster or other tragedy.
COUNTERFEIT PRODUCT	Counterfeit goods mimic original merchandise, right down to the trademarked logo, but are typically of inferior quality. This can result in a life-threatening health or safety hazard when the counterfeit item is medication or an auto part.
CREDIT CARD	This con typically involves impersonation of a bank or other credit card issuer. By verifying account information, con artists try to fool their targets into sharing credit card or banking information.
CREDIT REPAIR/ DEBT RELIEF	Scammers posing as legitimate service providers collect payment in advance with promises of debt relief and repaired credit but provide little or nothing in return.
CRYPTOCURRENCY	These scams involve the purchase, trade, or storage of digital assets known as cryptocurrencies. Often these scams involve fraudulent Initial Coin Offerings (ICOs), a type of fundraising mechanism in which a company issues its own cryptocurrency to raise capital. Investors are scammed into paying money or trading their own digital assets when the scammer has no intention of building a company. Cryptocurrency scams also involve scenarios in which investors store their cryptocurrencies with fraudulent exchanges.
DEBT COLLECTION	In this con, phony debt collectors harass their targets, trying to get them to pay debts they don't owe.
EMPLOYMENT	Victims of employment scams are led to believe they are applying or have just been hired for a promising new career when instead they have, in fact, given personal information or money to scammers for "training" or "equipment." In another variation, the victim may be "overpaid" with a fake check and asked to wire back the difference.
FAKE CHECK/ MONEY ORDER	In this con, the victim deposits a phony check and then returns a portion by wire transfer to the scammer. The stories vary, but the victim is often told they are refunding an "accidental" overpayment. Scammers count on the fact that banks make funds available within days of a deposit but can take weeks to detect a fake check.
FAKE INVOICE	This scam targets businesses. Scammers attempt to fool employees into paying for products that the business did not order and that may not even exist. Fake invoices are often for office supplies, website or domain hosting services, and directory listings.
FAMILY/FRIEND EMERGENCY	This scheme involves the impersonation of a friend or family member in a fabricated urgent or dire situation. The "loved one" invariably pleads for money to be sent immediately. Aided by personal details they've found on social media, imposters can offer very plausible stories to convince their targets.
FOREIGN MONEY EXCHANGE	In this scam, the target receives an email from a foreign government official, member of royalty, or a business owner offering a huge sum for help getting money out of the scammer's country. The victim fronts costs for the transfer, believing that they will be repaid.
GOVERNMENT GRANT	In this con, individuals are enticed by promises of free, guaranteed government grants. The only catch is a "processing fee." Other fees follow, but the promised grant never materializes.
HEALTH CARE, MEDICAID, AND MEDICARE	These schemes run the gamut, with many attempting to defraud private or government health care programs. The con artist is often after the insured's health insurance, Medicaid, or Medicare information to submit fraudulent medical charges or for purposes of identity theft.

APPENDIX A: Glossary of Scam Type Definitions

HOME IMPROVEMENT	In this con, door-to-door solicitors offer quick, low-cost repairs and then either take payments without returning, do shoddy work, or "find" issues that dramatically raise the price.
IDENTITY THEFT	Identity thieves use a victim's personal information (e.g., Social Security number, bank account information, and credit card numbers) to pose as that individual for their own gain. Using the target's identity, the thief may open a credit account, drain an existing account, file tax returns, or obtain medical coverage.
INVESTMENT	These scams take many forms, but all prey on the desire to make money without much risk or initial funding. "Investors" are lured with false information and promises of large returns with little or no risk.
MOVING	These schemes involve rogue moving services offering discounted pricing to move household items. They may steal the items or hold them hostage, demanding additional funds to deliver them to the new location.
ONLINE PURCHASE	These cons often involve purchases and sales, often on eBay, Craigslist, or other direct seller-to-buyer sites. Scammers may pretend to purchase an item only to send a bogus check and ask for a refund of the "accidental" overpayment. In other cases, if the scammer is the seller, they never deliver the goods.
PHISHING	These schemes employ communications impersonating a trustworthy entity, such as a bank or mortgage company, intended to mislead the recipient into providing personal information with which the scammer can gain access to bank accounts or can steal the recipient's identity.
RENTAL	Phony ads are placed for rental properties that ask for up-front payments. Victims later discover the property doesn't exist or is owned by someone else.
ROMANCE	An individual believing he/she is in a romantic relationship is tricked into sending money, personal and financial information, or items of value to the perpetrator.
SCHOLARSHIP	This con hooks victims, often students struggling with tuition costs, with the promise of government scholarship money, but the up-front "fees" never produce those much-needed funds. Sometimes a fake check does arrive, and the student is asked to wire back a portion for taxes or other charges.
SWEEPSTAKES, LOTTERY, AND PRIZE	This con fools victims into thinking they have won a prize or lottery jackpot but must pay up-front fees to receive the winnings, which never materialize. Sometimes this con involves a fake check and a request to return a portion of the funds to cover fees.
TAX COLLECTION	In this con, imposters pose as Internal Revenue Service representatives in the United States or Canada Revenue Agency representatives in Canada to coerce the target into either paying up or sharing personal information.
TECH SUPPORT	Tech support scams start with a call or pop-up warning that alerts the target to a computer bug or other problem. Scammers posing as tech support employees of well-known tech companies hassle victims into paying for "support." If the victim allows remote access, malware may be installed.
TRAVEL AND VACATION	Con artists post listings for properties that are not for rent, do not exist, or are significantly different from what's pictured. In another variation, scammers claim to specialize in timeshare resales and promise they have buyers ready to purchase.
UTILITY	In this con, scammers impersonate water, electric, and gas company representatives to take money or personal information. They frequently threaten residents and business owners with deactivation of service unless they pay immediately. In another form, a "representative" may come to the door to perform "repairs" or an "energy audit" with the intent of stealing valuables.
YELLOW PAGES/ DIRECTORY	This con targets businesses, attempting to fool them into paying for a listing or ad space in a nonexistent directory or "Yellow Pages." In some cases, the directory technically exists, but is not widely distributed and a listing is of little or no value—these directories are essentially props in the scammer's ploy.