FRAMEWORK FOR A TAXONOMY OF FRAUD

A joint collaboration of the Financial Fraud Research Center at the Stanford Center on Longevity and the FINRA Investor Education Foundation

July 2015

STANFORD CENTER ON LONGEVITY

FINRA Investor Education FOUNDATION

Michaela Beals
Marguerite DeLiema
Martha Deevy

longevity.stanford.edu/financial-security

Acknowledgements

The development of the Framework for a Taxonomy of Fraud was coordinated by the Financial Fraud Research Center at the Stanford Center on Longevity, the FINRA Investor Education Foundation, and the Bureau of Justice Statistics in the United States Department of Justice. This report was prepared by Michaela Beals and Marguerite DeLiema under the direction of Martha Deevy at the Financial Fraud Research Center, with significant input from the *Taxonomy of Fraud* working group and a panel of extended reviewers. Special thanks to Gary Mottola at the FINRA Investor Education Foundation and Michael Planty and Lynn Langton at the Bureau of Justice Statistics for guidance and support. The authors would also like to thank our research assistant, Sydney Krueger, for her help coding consumer complaint data and reviewing the report.

Working Group Members

- Keith Anderson – Economist, Federal Trade Commission
- Robert Anguizola – Assistant Bureau Chief, Enforcement Division, Federal Communications Commission
- Michaela Beals – Research Analyst, Financial Fraud Research Center, Stanford Center on Longevity
- Martha Deevy –Director, Financial Security Division and Financial Fraud Research Center, Stanford Center on Longevity
- Marguerite DeLiema – Postdoctoral Researcher, Financial Fraud Research Center, Stanford Center on Longevity
- Kristy Holtfreter – Associate Professor and Director of Graduate Programs, School of Criminology and Criminal Justice, Arizona State University
- Dominika Jaworski –Research Associate, Financial Security Division, Stanford Center on Longevity
- Sara Kern – Associate Professor of Accounting, Gonzaga University
- Christine Kieffer – Senior Director, FINRA Investor Education Foundation
- Lynn Langton – Statistician, Bureau of Justice Statistics, United States Department of Justice
- Gary Mottola – Research Director, FINRA Foundation
- Michael Planty – Chief, Victimization Statistics, Bureau of Justice Statistics, United States Department of Justice
- Patricia Poss – Senior Attorney, Division of Marketing Practices, Bureau of Consumer Protection, Federal Trade Commission
- Michael Reisig – Professor, School of Criminology and Criminal Justice, Arizona State University
- Richard Riley – Professor of Public Accounting, West Virginia University, Director of Research, Institute for Fraud Prevention
- Doug Shadel – State Director, AARP Washington
- Roger Tourangeau – Vice President and Associate Director, Westat

Extended Review Panel

- Debbie Deem – Victim Specialist for Los Angeles, Federal Bureau of Investigation

- Owen Donley – Chief Counsel, Office of Investor Education and Advocacy, Securities and Exchange Commission
- Lois Greisman – Associate Director, Division of Marketing Practices, Federal Trade Commission
- Dana Hermanson – Professor of Accounting, Kennesaw State University
- Michael Herndon – Consumer Outreach Officer, Commodity Futures Trading Commission
- Andi McNeal – Director of Research, Association of Certified Fraud Examiners
- Jerry O'Farrell – Inspector in Charge, Criminal Investigations, US Postal Inspection Service
- Nicole Piquero – Professor of Criminology, University of Texas, Dallas
- Lori Schock – Director of the Office of Investor Education and Advocacy, Securities and Exchange Commission
- Terry Thome – Deputy Chief Inspector of the Eastern Field Operations, US Postal Inspection Service
- Richard Titus – retired Program Manager, National Institute of Justice
- John Warren – Vice President & General Counsel, Association of Certified Fraud Examiners
- Johan van Wilsem – Associate Professor Of Criminology, Leiden University, The Netherlands
- Judy van Wyk – Associate Professor of Sociology, University of Rhode Island

Table of Contents

I. Background

The need for a classification system

Financial fraud is a major problem for individuals and for society, but our understanding of the scope of the problem is hampered by a lack of official statistics. Key sources of crime statistics in the United States, including the Bureau of Justice Statistic's *National Crime Victimization Survey* (NCVS) and the Federal Bureau of Investigation's *Uniform Crime Reports*, have historically focused on traditional property crimes like burglary and larceny. While there is a recognized need to incorporate emerging crimes like financial fraud into these key surveys of crime, the first step is to create an agreed upon and operationalized definition of fraud.

Currently, there is a lack of a clear definition for the term "fraud." Much of fraud research has focused on fraud against governments and organizations, which is distinct from fraud against individuals, both in its methods and in its players. The lack of a clear definition has allowed individual financial fraud to remain relatively overshadowed and overlooked.

Because no systematic categorization currently exists, researchers and practitioners have classified fraud types based on different characteristics, including communication method (e.g., cyber fraud, mail fraud), product marketed (e.g., lottery fraud, securities fraud), strategy employed (e.g., advance fee fraud, overpayment fraud), group targeted (e.g., elder fraud), and/or fraudster characteristics (e.g., employee fraud, occupational fraud). This has led to a proliferation of overlapping and often confusing definitions and categorizations that affect fraud prevalence estimates as well as our understanding of the mechanisms and consequences of fraud.

The Taxonomy of Fraud Project

Genesis of the Project & Tasks Accomplished to Date

To address the need for a fraud classification system, the Financial Fraud Research Center, a joint project of the Stanford Center on Longevity and the FINRA Investor Education Foundation (FINRA Foundation), collaborated with the Bureau of Justice Statistics to develop a standardized fraud classification scheme. The purpose was to group and organize fraud types meaningfully and systematically into a definitional framework that can be translated into survey questions and administered with the *National Crime Victimization Survey*. The survey will be used to determine the current prevalence of individual financial fraud and how prevalence rates change over time. As such, an initial filter for this project was to limit the classification to fraud types and attributes that could reasonably be identified and reported by victims or that are of interest to researchers and fraud investigators.

In addition to informing the development of a consumer fraud survey, the taxonomy has wider applications in the field. The standardized coding scheme will improve consistency in fraud measurement so that findings can reasonably be compared across time and across groups. The taxonomy can easily be modified to include additional attributes about fraud incidents that are important to law enforcement and fraud investigators. Researchers can also choose which code dimensions they are interested in analyzing for their own study purposes. Furthermore, the taxonomy is useful in helping to conceptualize the problem of fraud, delineate the boundaries between fraud and other types of misleading or deceptive financial transactions, and to evaluate how fraud evolves over time.

Although researchers and practitioners have long recognized the need for an individual financial fraud classification system, this specific project is an outgrowth of a conference supported by the FINRA Foundation and hosted by the Financial Fraud Research Center entitled, *The True Impact of Fraud – A Roundtable of Experts*[1] held in Washington, DC in the spring of 2014. At this conference, experts gathered to discuss ways to improve the measurement of fraud's impact. One of the key themes of the conference was that a taxonomy of fraud would be extremely beneficial to the field.

The project began with a workshop-style meeting in Washington DC in January 2015 that focused on identifying the initial dimensions and organizational structure of the taxonomy. The *Taxonomy of Fraud* Working Group consisted of a small number of fraud and measurement experts representing government, academic, and nonprofit organizations. Over the course of the workshop and several conference-call discussions, the group developed the initial draft of the taxonomy described in this report.

The taxonomy and associated report were also evaluated by an extended review panel consisting of a wider scope of fraud and measurement researchers and practitioners. Input from the extended review panel helped refine the taxonomy by addressing potential areas of overlap or confusion. The panel also offered organizational suggestions to improve comparability and integration with existing typologies and classification schemes.

As a final validation step to assess comprehensiveness and applicability, the taxonomy was tested using consumer complaint data from the Federal Trade Commission's (FTC) Consumer Sentinel Network database. Three-hundred consumer fraud complaint cases were classified using the taxonomy coding scheme. Attribute tags were applied if specific information about the victim, perpetrator, advertising method, and/or method of transfer was reported by the consumer. This validation step using FTC data identified gaps in the taxonomy and areas where clearer definitions were needed. The objective was to ensure that the taxonomy captured the full range of common scams against consumers and that the definitions reflected consumers' experiences. Based on the consumer complaint data, parts of the taxonomy were reorganized and amended with additional fraud types.

Next Steps

In the next phase of the project, the FINRA Foundation will fund the development of survey items based on the taxonomy, with the goal of including these items in a supplement questionnaire to the core *National Crime Victimization Survey* (NCVS). The NCVS is administered biannually by the Bureau of Justice Statistics to over 90,000 households in the United States. The fraud supplement will be used to determine the annual prevalence of specific types of fraud and how these rates change over time.

This report and the associated victimization survey focus primarily on fraud targeting individuals. To expand the scope of the project, the Financial Fraud Research Center will collaborate with members of the Association for Certified Fraud Examiners (ACFE) to refine the taxonomy by creating a full classification scheme for fraud targeting for-profit and non-profit organizations, such as asset misappropriation and corruption, as well as fraud targeting government regulations and policies, such as

[1] Conference proceedings are available at: http://fraudresearchcenter.org/2014/06/the-true-impact-of-fraud-a-roundtable-of-experts-washington-dc-2014/

immigration fraud and welfare fraud. While these types of crime have a place in the current taxonomy, the section requires further development and input from experts in those areas.

II. Developing a Taxonomy of Fraud

This taxonomy is modeled after the international crime classification system proposed in the UN report, *Principles and Framework for an International Classification of Crimes for Statistical Purpose*,[2] prepared by the UNODC/UNECE task force on crime classification. The UN report outlines the main principles of an international crime classification scheme and provides an example framework. Wherever possible, we adopted the UNODC/UNECE guidelines and terminology.

General principles of classification

As noted in the UN report, a classification scheme is an "exhaustive and structured set of mutually exclusive and well-described categories."[3] The authors note that this definition references four distinct elements that serve as principles for classification:

- Exhaustiveness: The framework should include every possible manifestation of the phenomenon under study.
- Structure: The classification should include meaningful hierarchical organization, with similar values grouped together.
- Mutual exclusiveness: Each manifestation of the phenomenon under study should be assigned to one and only one category, precluding the possibility of overlaps.
- Description: Each incident must be described with enough detail to allow assignment to the appropriate category.

The principles were slightly modified for practical application, but serve as the basis for our Taxonomy of Fraud. Each principle and its application to the taxonomy are outlined in detail following the description of the framework elements.

[2] UNODC/UNECE, 2012, *Principles and Framework for an International Classification of Crimes for Statistical Purpose*, Report of the UNODC/UNECE Task Force on Crime Classification to the Conference of European Statisticians, available at www.unodc.org/documents/data-andanalysis/statistics/crime/Report_crime_classification_2012.pdf

[3] United Nations Statistical Commission, Standard Statistical Classifications: Basic Principles. Paper presented at Thirtieth session, New York, 1-5 March 1999 cited in *ibid*.

III. Framework elements

The unit of classification

This framework was developed for future data collection using population-based victimization surveys. Events captured by these surveys typically use a behavioral or event-based approach. Survey respondents are asked to describe an event, focusing on the main attributes of the incident. The fraud taxonomy is similarly event-based and attribute-based.

The unit of analysis is the fraudulent “act/event/incident” that meets the definition of fraud presented below. The incident is coded within the taxonomy based on characteristics such as the target of the fraud, the product or service fraudulently offered, and the specific type of scheme.

The taxonomy is intended to categorize instances of completed or successful fraud, rather than attempted fraud. To satisfy this requirement, the victim must lose money in the transaction. We recognize that even attempted fraud can have serious consequences for victims, such as lost time, confidence, and feelings of insecurity. We also recognize that tracking fraud attempts can inform agencies about who is being targeted and where efforts are needed to educate and protect consumers; however, we are interested in using this taxonomy to gather prevalence data on successful fraud. It can still be used to collect data on fraud attempts should other agencies or researchers wish to capture these incidents. This could be accomplished by adding an attribute tag to differentiate successful fraud from attempted fraud.

As a starting point for developing this taxonomy, we used the following working definition for fraud based on Titus, Heinzelmann, and Boyle’s[4] definition, in addition to contributions from the taxonomy working group:

Intentionally and knowingly deceiving the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain.

One of the challenges to developing a valid taxonomy and definition is determining the boundaries of fraud. Even legitimate companies and sellers may overstate the benefits of their products and services to convince consumers to buy, and advertisements at times make deceptive and misleading claims. Moreover, some incidents that consumers label as fraud are actually just poor customer service or the result of a miscommunication. While these distinctions can be ambiguous, we argue that the general intent of scam artists is to make money off of consumers by deliberately giving them nothing of value or something of considerably less value than what was promised. Comparatively, while legitimate sellers sometimes market their products and services in deceptive and misleading ways, they generally do not intend to take a customer’s money and provide nothing of value in return.

How we intend to differentiate fraud from other forms of consumer deception in this taxonomy is that in cases of fraud, scam artists *knowingly* and *deliberately* deceive consumers by convincing them to engage in a transaction that no reasonable person would agree to if he or she had been told the truth. To satisfy

[4] Titus, R. M., Heinzelmann, F., & Boyle, J. M. (1995). Victimization of persons by fraud. *Crime & Delinquency, 41*(1), 54–72.

this parameter, we aimed to avoid classifying unfair business practices and sellers' mistakes as fraud if they were not intentionally designed to benefit the seller at the consumer's expense, yet these are often difficult distinctions to make. For example, failing to honor a refund or warranty policy, failing to communicate the details of a contract, and failing to ship an item the consumer paid for may be labeled as fraud or poor customer service, depending on the specifics of the transaction. To minimize the possibility of "false positives"—labeling an incident as fraud when it is not—a concerted effort was made to ensure that the taxonomy and related victimization survey do not count incidents that do not meet our fraud criteria. And to minimize the possibility of false negatives—omitting true incidents of fraud—the taxonomy and survey include a wide range of common scams that are carefully described in this report.

In our conceptualization of fraud in the taxonomy, the victim must be deceived or persuaded into participating in the fraudulent transaction. As such, we have intentionally excluded identity theft from the framework because victims are not persuaded to disclose personal information based on the belief that they will get something in return. Rather, identity theft**—**and related crimes like credit card fraud**—**is akin to other forms personal theft. The difference is that the valuable "good/property" stolen is the victim's identity and/or financial account information. This theft of information typically occurs beyond the victim's consent, knowledge, and control.

Furthermore, the distinctions between identity theft and fraud, as defined in this report, are modeled after other surveys and are recognized by fraud investigatory agencies. For example, the FTC's prevalence surveys on consumer fraud in the United States do not ask respondents to report incidents of stolen identity or stolen credit card information. This information is captured in the identity theft supplement of the *National Crime Victimization Survey*.

While we recognize that there may be some areas of overlap and that most consumers are not aware of the differences between fraud and identity theft, and thus report these incidents to the same complaint agencies, we have decided to exclude identity theft from the taxonomy based on the distinctions explained above.

Key Organizational Concepts and Attributes

To determine the important attributes to include in a crime classification scheme, the UN task force conducted background research to investigate existing schemes from several different countries. They found that, in addition to the main variable of "type" of offense, countries also reported using other descriptive variables, including the date, time, location of the offense, the means (modus operandi), the objects or weapons used, and the nature of damage caused. Many also collected basic suspect/offender and victim data, such as age, sex, and race.

Using this information, the UN task force created a list of attributes that should be included in an international crime classification. Their list included: the "target" of the act, the "seriousness" of the act, the "intent" of the perpetrator, the "modus operandi" of the act, the "degree of completion" of the act, the "degree of co-responsibility" of other people involved, the "sex and age" of victims and perpetrators, and the "policy area" of the act.[5]

With this list as a foundation, we created a list of attributes that are relevant to a fraud classification scheme. These attributes represent what information should be captured in the taxonomy of fraud, either through categorization within the taxonomy hierarchy (framework levels), or through additional descriptive information that can be applied to the incident (attribute "tags").

Below are the concepts and attributes used to organize the taxonomy and qualify fraud incidents. The first three concepts are used to place (categorize) the event in the appropriate location within the framework hierarchy.

- Target: Describes the main entity against whom/which the fraud is directed. The focus of this taxonomy is fraud committed against individuals, but the structure also indicates where fraud against organizations and groups could be expanded in the future.
- Expected benefit/outcome: The victim's expected or promised reward, benefit, or outcome of the fraudulent transaction (e.g., expected investment returns, expected product or service to be received, expected prize, expected charitable giving, expected debt owed) is used to classify the fraud type within the taxonomy framework.
- Specific type of fraudulent item/transaction/relationship: Further specification of the fraud type relates to what specifically about it was fraudulent. For example, what type of investment, product, service, or charity was misrepresented or used to deceive the victim? For certain categories of fraud, this pertains to the type of relationship (friendship, romantic, familial) that was exploited.

The following attributes are not used to organize the taxonomy structure, but can be applied as "tags" to provide further information about the event.

- Seriousness: In this taxonomy, the seriousness of the fraud is captured by the dollar loss value and the duration of the incident (identified with dollar loss categories and duration tags).
- Victim and perpetrator characteristics: Demographic (e.g., sex and age) and other characteristics (e.g., veteran status) of the victim and perpetrator provide context to the full nature of the event. These attributes also provide the necessary information to identify certain types of fraud, like *elder fraud* and *veteran fraud*. They are also useful to classify the relationship of the perpetrator to the victim, such as *family member* or *caregiver*, and whether the target has been victimized more than once (repeat victim).
- Method of advertising the fraud: Describes how the fraud was promoted to victims. Possible values include: the internet/email, texting/direct message, mailed advertisement, TV and radio, telemarketing, and in person. Capturing this information allows for the identification of telemarketing fraud and some types of cyber fraud, and helps determine jurisdictional relevance (e.g., mail fraud, wire fraud).

[5] UNODC/UNECE, 2015, *International Classification of Crime for Statistical Purposes; Version 1.0*, Report of the United Nations Office on Drugs and Crime, available at https://www.unodc.org/documents/data-and-analysis/statistics/crime/ICCS/ICCS_final-2015-March12_FINAL.pdf

- Purchase Setting: Describes the setting in which the fraudulent transaction took place or how the victim responded to the scam. Possible values include: computer via the Internet, mail, telephone, brick and mortar store, or person to person sale. This information is useful in identifying certain types of cyber fraud and jurisdictional relevance (e.g., mail fraud, wire fraud). It also indicates promising areas for intervention.
- Method of money transfer: Describes the precise mechanism by which the victim paid money to the fraudster. This tag seeks to answer the question of how the money moved from the possession of the victim to the possession of the fraudster. Possible values include: credit card, debit or ATM card, cash, personal check, mobile or online payment application (such as PayPal, Square, Venmo, Google Wallet), money order, wire funds, telephone account, prepaid cards, or Bitcoin. Information about how the money was transferred from victim to the perpetrator allows for identification of specific types of cyber fraud and helps determine jurisdictional relevance (e.g., mail fraud, wire fraud). It also identifies what payment systems are preferred by scam artists and may need better security systems to protect victims.

We recognize that some of these tags may change as new technologies emerge for transferring money and information. These mechanisms can be integrated as new attribute tags in future iterations of the taxonomy. The following attributes are not included as stand-alone tags in the taxonomy, but they can be identified by the presence of other tags (or combinations of tags) described above. Furthermore, additional tags can be added if investigators wish to use the taxonomy to classify fraud schemes that are used to finance other criminal activity, such as money laundering, and fraud perpetrated by organized criminal groups.

- Internet or cyber fraud: Describes if the fraud was facilitated by the use of the computer or internet. The category of internet or cyber fraud can be determined by the presence of one or more of the following: the fraud was advertised via the Internet or email, the fraudulent transaction took place over the internet (e.g., an online auction), or an online or mobile payment mechanism was used to transfer the money (e.g., Apple Pay).
- Mail fraud: Describes if the fraud would be classified as the federal offense of mail fraud. Any scam artist who uses the U.S. mail in an attempt to commit fraud can be prosecuted under the federal mail fraud law. The category of mail fraud can be determined by the presence of one or more of the following: the fraud was advertised through direct mail, the fraudulent transaction took place using the mail system (e.g., check or money order sent through the mail), or the mail was used to conceal and/or continue false pretense (e.g., statement, bill of sale, or purchase agreement sent through the mail).
- Wire fraud: Describes if the fraudulent transaction involved using a cell phone or a computer—or any device that sends information across state lines, which is classified as the federal offense of wire fraud. The category of wire fraud can be determined by the presence of one or more of the following: the fraud was advertised over the Internet, TV, radio, or telephone; the fraudulent transaction took place using the Internet or telephone; or the money was transferred using a mobile payment mechanism or telephone account.
- Policy area: Some acts of fraud have particularly high policy relevance which are reflected in the taxonomy. For example, elder fraud and cyber fraud have high policy relevance, so the taxonomy structure allows for easy tallying of these types of fraud.

Framework levels

The main structure (grid) of the taxonomy is organized on the basis of various levels (vertical organization) and categories within those levels (horizontal organization) based on various attribute designations. Each level is described in brief below and in detail in Section V.

Level 1: The highest (broadest) level of the taxonomy consists of just two categories grouped based on the target of fraud. The categories are as follows: 1) Fraud against an *individual*, and 2) Fraud against an *organization*. This level of the taxonomy is intended to be both mutually exclusive and exhaustive, so that all manifestations should fit into one and only one category.

Although this taxonomy structure allows for integration with other typologies addressing fraud against organizations, the focus of this project is individual financial fraud. We have therefore indicated where some types of fraud against organizations would fit in the proposed taxonomy (Category 2), but detailed classification is beyond the scope of the current project. The Financial Fraud Research Center is collaborating with the Association of Certified Fraud Examiners (ACFE) on a corollary project to further develop the section concerning fraud against organizations.

Level 2: This level consists of seven sub-categories of Individual Financial Fraud based on the expected benefit or expected consequence of the transaction. The seven level 2 categories are listed below and are described in more detail in Section V of this report. This level is intended to be comprehensive and mutually exclusive, such that all possible examples of individual financial fraud committed against persons in the general public[6] should fall into one and only one of the below seven categories.

1) Consumer Investment Fraud: expected benefit is investment returns. Examples include securities fraud, Ponzi schemes, commodities fraud, Hollywood film scams, etc.
2) Consumer Products and Services Fraud: expected benefit is a consumer product or service. Examples include worthless or non-existent products (dietary supplements), worthless services (phony insurance, credit repair scams, and unnecessary home repairs) and unauthorized billing. Also included in this category are scams where a consumer is sold a vacation, tickets to an event, or rental housing that does not exist or is not provided as promised.
3) Employment Fraud: expected benefit is employment. Examples include business opportunities, work-at-home scams, government job placement scams, and nanny scams, etc.
4) Prize and Grant Fraud: expected benefit is winning some sort of prize, grant, lottery, or other windfall of money. Examples include prize promotions/sweepstakes, foreign and domestic lottery fraud, inheritance scams, government grant offers, and Nigerian letter scams.
5) Phantom Debt Collection Fraud: expected benefit is avoiding the consequences of failing to pay debts that the victim did not previously know were owed (and that turn out to be fake). Examples include government debt collection scams (court impersonation scam, IRS back taxes owed scam), and other scams in which fraudsters demand payment for false debt owed to lenders or businesses (obituary scam, fake medical debt, fake loan debt collection).

[6] Note that we do not consider scams and fraud committed between criminals within the scope of this taxonomy.

6) Charity Fraud: expected benefit is contributing to a charity or non-profit organization. Examples include bogus natural disaster relief, law enforcement charities, children's organizations, and personal crowdfunding sites for bogus causes.
7) Relationship and Trust Fraud: expected benefit is fostering or continuing a personal and sometimes intimate relationship. Examples include friends/relatives imposter scams (grandparent scam) and in person or online romance scams.

Level 3: This level of the proposed framework consists of further sub-types of the level 2 fraud categories. These sub-types are grouped based on the attribute of "type of fraudulent item/transaction/relationship" (type of investment, product/service, charity, etc.).

For example, level 3 sub-divides Consumer Investment Fraud into "Securities Fraud" and "Commodities Fraud" based on the type of investment. Similarly, level 3 divides Relationship & Trust Fraud into categories based on what type of relationship is being exploited (e.g., relative imposter scam, romance scam).

Whereas higher order levels of the taxonomy are intended to be complete, level 3 is not comprehensive. At this level of specificity, new fraud types are constantly evolving in tandem with new technology and market trends. Thus, level 3 designates several "other" categories to account for specific fraud types not listed or new fraud types that may arise in the future.

Levels 4 and 5: These levels consist of further sub-types or common examples of higher order fraud types. Like level 3, levels 4 and 5 are not intended to be exhaustive and include "other" categories to account for new fraud types that are not captured in the current taxonomy.

Coding

Following the UN task force classification system, each fraud type is assigned a numeric code that relates to its placement within the taxonomy grid. The first numeral reflects which of the highest category levels the act/event falls into, with subsequent numerals indicating further sub-categories in successive levels. Since there are 5 possible levels, the code can have up to 5 numerals, with a greater number of numerals indicating a greater level of specificity of the fraud type. For example, the broad level 1 category of "Individual Financial Fraud" is coded as (1), the level 2 sub-category "Consumer Investment Fraud" is (1.1), a level 3 sub-category is "Securities Fraud" coded as (1.1.1), the level 4 sub-category ,"Equity (stock) investment fraud," is (1.1.1.1), and the specific scam "Penny stock fraud" is coded as (1.1.1.1.1). Section V describes every sub-type and the corresponding classification number in detail. All unspecified fraud types classified as "other" end in .99. This numbering system allows new types of fraud to be added to the framework as needed while preserving the numeric codes for "other" fraud types.

Secondary incidents

In some cases an incident of fraud leads to a subsequent, related incident, such as when a consumer agrees to an advance fee loan, and then is contacted by scam artists alleging he owes money to pay back that same bogus loan. For survey purposes, only the initial incident will be recorded if it occurred within the timeframe of interest; yet, using this taxonomy, both incidents can be separately coded.

Attribute tags

In addition to attributes that determine where an incident is placed within the taxonomy structure, additional attribute information can be applied to the description of the act/event with the use of attribute “tags.” Descriptive information about the victim and the perpetrator (age, sex, nature of the relationship) is captured through attribute tags, as well as additional information about the fraudulent incident, such as how the fraud was advertised (how the information reached the victim), the setting in which the transaction took place, the method that money was transferred, and how much money was lost.

In general, these attributes can be applied across all classification levels and categories, and more than one tag can be applied to a particular incident. The tags are organized into three groups: 1) Incident tags; 2) Victim tags; and 3) Perpetrator tags. These tags provide additional descriptive information that is not captured by where the fraud is placed in the taxonomy framework, but is important for understanding the full context of the fraud or its jurisdictional (e.g., wire fraud, mail fraud) or policy relevance (e.g., elder fraud). All tags are listed below and described in detail in Section V.

Incident Tags

General Incident Tags

- AF - Affinity fraud
- PS - Pyramid scheme
- PZ - Ponzi scheme
- IG - Impersonated Government official
- PD - Pump & dump scheme
- HM - Health or medical related fraud
- CS - Continuity scam (aka, Negative option scam)
- OV - Overpayment fraud
- CP - Counterfeit payment instrument

Method of Advertising the Fraud

- Ad:IE - Internet, email
- Ad:TX - Text/direct message
- Ad:DM - Direct mail
- Ad:TVR - TV or radio
- Ad:T - Telemarketing
- Ad:P - In person

Purchase Setting

- PS:I - Computer via the Internet
- PS:M - Mail
- PS:T - Telephone
- PS:S - Store (brick and mortar)
- PS:P - Person to person

Method of Money Transfer

- MT:CC - Credit card
- MT:DC - Debit/ATM card
- MT:C - Cash

- MT:PC – Personal check
- MT:M – Mobile/online payment application
- MT:MO - Money order
- MT:W - Wire funds
- MT:T - Telephone account
- MT:PP - Prepaid cards
- MT:B - Bitcoin

Dollar loss categories

Duration of fraud

Victim Tags

- MV - Male Victim
- FV - Female Victim
- EV - Elder Victim (65+)
- VV - Veteran Victim
- CIV - Cognitively Impaired Victim
- RV - Repeat Victim
- RA - Victim reported fraud to authorities

Perpetrator Tags

- MP - Male Perp
- FP - Female Perp
- IP - Intimate Partner Perp
- FP - Family member Perp
- CP - Caregiver Perp

As this taxonomy represents a "living" framework, several other attribute tags could be included in the future, including the geographic location of the act, the use of identity theft to commit the fraud, and the psychosocial impact upon the victim. Other attributes in the UN report that can be added are whether the fraudulent act was part of a larger scheme to launder money and whether the perpetrator was part of an organized criminal group.

Coding

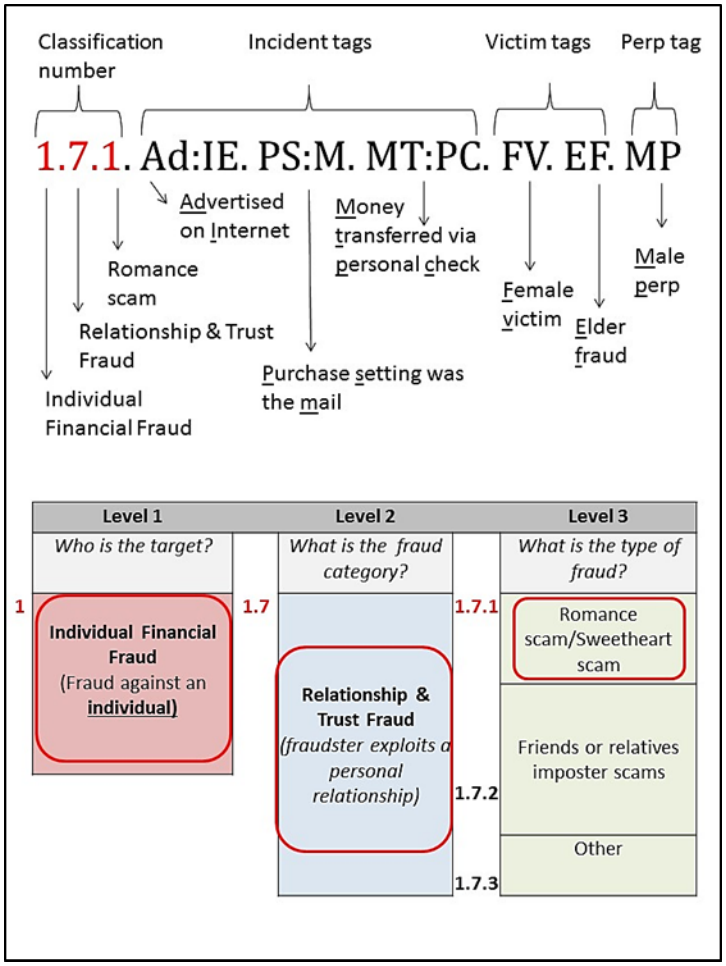
Each attribute tag should be placed the end of the numeric code that indicates where the incident belongs in the taxonomy hierarchy. Using the example above, a "Penny stock fraud" is coded as (1.1.1.1.1). If information is available indicating that the victim was male and targeted based on his church membership, and that the perpetrator was male, the following attribute tags would be added: AF (affinity fraud), MV (male victim), and MP (male perpetrator), resulting in the following code: 1.1.1.1.1.AF.MV.MP.

Example scenario

For clarification of the coding assignment process, consider the following case:

Mary, age 67, reports that her online relationship started out as a friendship. Mary found the man on a social networking site. The two "lovers" would tell each other about themselves and later spoke to one another over the phone. He told her he was stuck in Nigeria and needed help to fly home. Mary started mailing checks to help her lover. She blew through her own money and eventually had to start taking out loans to help him.

This event would be coded in the proposed taxonomy as: 1.7.1.Ad:IE. PS:M. MT:PC. FV. EF. MP. The taxonomy classification number 1.7.1 indicates that the act is coded as Individual Financial Fraud (1) → Relationship & Trust Fraud (1.7) → Romance Scam (1.7.1). The additional tags indicate that the fraud was advertised or promoted on the Internet (Ad:IE), the purchase setting was the mail (PS:M), the precise method of money transfer was personal check (MT:PC), the victim was female (FV), the incident is considered elder fraud (EF), and the perpetrator is male (MP). Note that this scenario would be considered cyber fraud because the fraudulent transaction was facilitated by the use of the internet (as indicated by the Ad:IE tag). It could also be considered mail fraud since the money was sent via the postal system (as indicated by the PS:M tag).


Classification number
Incident tags
Victim tags
Perp tag
1.7.1. Ad:IE. PS:M. MT:PC. FV. EF. MP
Advertised on Internet
Money transferred via personal check
Romance scam
Female victim
Male perp
Relationship & Trust Fraud
Elder fraud
Purchase setting was the mail
Individual Financial Fraud

	Level 1		Level 2		Level 3
	Who is the target?		*What is the fraud category?*		*What is the type of fraud?*
1	**Individual Financial Fraud** (Fraud against an **individual)**	1.7	**Relationship & Trust Fraud** *(fraudster exploits a personal relationship)*	1.7.1	Romance scam/Sweetheart scam
				1.7.2	Friends or relatives imposter scams
				1.7.3	Other

IV. Revisiting the principles of classification: Practical application

Exhaustiveness:

Under the principle of exhaustiveness, it is necessary to include all possible acts or events that could be considered fraudulent. However, this principle must be balanced with the practicality of including all types of fraud. Because fraud is always evolving with new forms frequently arising, the more specific levels of the taxonomy are not intended to be exhaustive; however, the higher-level categories (levels 1 and 2) should be sufficiently broad to accommodate all types of fraud.

Structure:

As noted in the UN report, too many hierarchical levels in a classification system can hamper manageability. Thus, the taxonomy currently has seven broad categories of Individual Financial Fraud and a total of five possible levels of specificity. To reduce complexity, some categories do not include level 5 examples when level 4 specificity is sufficient. The fraud victimization survey based on this taxonomy will incorporate skip patterns to eliminate the need for respondents to provide answers on every question, thereby reducing participant burden. Moreover, the terms used to label different fraud types will not necessarily be the same terms used in the victimization survey. Many victims do not see themselves as such, and thus would not report losing money in the "IRS back taxes scheme" or by investing in "commodity pool fraud", for example. Thus, survey questions will be designed to focus on other characteristics of the incident such as how the victims were contacted or how they learned about the offer, what they expected but did not receive, and how much money was lost.

Mutual exclusiveness:

Using the current overlapping definitions of types of fraud, one incident has the potential to be categorized in several different ways. For example, an incident in which a victim receives an email saying she has won a prize and needs only pay a small administrative fee for processing could be categorized as a prize promotion scam or an internet scam (cyber fraud). In order to avoid ambiguity in these overlapping scenarios, the classification scheme was designed to break down the constituent elements of the incident, code them separately, but still link them together in the final description of the event. In the above example, this is accomplished by categorizing the event in the prize promotion/sweepstakes category (1.4.1) and adding an attribute tag that indicates the deception was facilitated over the Internet (Ad:IE) and is therefore cyber fraud as well. The salient point is that this classification scheme avoids overlap in the fraud subtypes but can still capture discrete elements of the act and other important information.

Note: Because the taxonomy is organized hierarchically with nesting levels, the principle of mutual exclusiveness only applies to the vertical organization of fraud types. By design, there is overlap moving left to right from the broad category to the more specific nested category; however, an incident should only have the potential to be placed in a single category within a vertical level.

Description:

Each incident must be defined with enough detail to allow assignment to the appropriate category. As described above, this descriptive information is assessed on the basis of various "attributes." Differences in attributes serve as the basis for categorizing fraud types into particular categories. Other attributes related to the fraud, such as how the money was transferred, determine which attribute tags to apply.

V. Detailed description of fraud codes and tags

Classification Categories

(1) Individual Financial Fraud

This refers to intentionally and knowingly deceiving the victim by misrepresenting, concealing, or omitting facts about promised goods, services, or other benefits and consequences that are nonexistent, unnecessary, never intended to be provided, or deliberately distorted for the purpose of monetary gain.

1.1 Consumer Investment Fraud

Investors gain and lose money in financial markets for a variety of legitimate reasons, yet the following definitions refer to investment fraud, where someone knowingly misleads an investor on the basis of false information. While many investment vehicles listed below have legitimate versions, they can also be used in investment scams where the earnings are grossly misrepresented or the investment itself is nonexistent. This broad category includes schemes in which perpetrators target victims with false promises of high financial returns in exchange for investing in securities, stakes in oil drilling ventures, precious metals. Forex, other commodities, and real estate investments. This category is further subdivided on the basis of the type of investment: securities fraud, commodities trading fraud, and other investment opportunities.

1.1.1 Securities fraud - Investment fraud dealing with securities, which are tradable financial assets in the form of an ownership position in a publicly-traded corporation (stock/equity), or a creditor relationship with governmental body or corporation (bond/debt). This category of investment fraud is further sub-divided into equity investment fraud, debt investment fraud, and other securities fraud.

1.1.1.1 Equity investment fraud - A type of securities fraud in which the fraudulent investment vehicle is equity or stock in a publically-traded corporation. Examples include penny stock fraud, high-yield investment fraud, and other general stock frauds.

1.1.1.1.1 Penny stock fraud - Also known as Microcap stock fraud, this is a form of securities fraud involving stocks of "microcap" companies, generally defined in the United States as those with a market capitalization of under $250 million. Many microcap stocks are penny stocks, which the SEC defines as a security that trades at less than $5 per share, is not listed on a national exchange, and fails to meet other specific criteria. A common example is a pump & dump scheme, in which promoters hype up investor sentiment in a little-known or unknown stock. New investors rush in, thus "pumping" up its price. Once shares are inflated, insiders then "dump" their shares at a huge profit and leave investors with large losses.

1.1.1.1.2 Pre-IPO scam - This is a type of securities fraud that deals in the sale of “pre-IPO” shares. The company might not exist—or, if it does, the promoter might be offering shares he doesn’t have or that he acquired in a questionable transaction. The fraud could also involve misrepresentations about the company and its prospects, including the likelihood, timing, and pricing of any potential IPO.

1.1.1.1.3 High-yield investment program (HYIP) fraud - These are unregistered investments created and promoted by unlicensed individuals. Typically offered online, HYIPs dangle the contradictory promises of safety coupled with high, unsustainable rates of return—20, 30, 100 or more percent per day—through vague or murky trading strategies. According to law enforcement cases, many operate as Ponzi schemes.

1.1.1.1.4 REIT (Real Estate Investment Trust) fraud - A type of securities fraud that deals with real estate investment trusts (REIT), a security that sells like a stock, but invests in large-scale real estate. A corporation will own and manage a portfolio of properties or mortgages, and investors can buy shares.

1.1.1.1.5 Oil & gas exploration scam - This type of investment fraud often starts in so-called "boiler rooms," where skilled telemarketers use high pressure sales tactics to convince an individual to invest in companies specializing in oil and gas exploration. Once they have the money, scam artists pay themselves first, often using funds to pay personal expenses. In the end, only some (if any) of the money is invested in an actual oil or natural gas well.

1.1.1.1.6 Alternative energy company scam - In this type of investment fraud, scam artists offer large gains for investing in companies purportedly involved in developing or producing alternative, renewable, or waste energy products.

1.1.1.1.99 Other equity (stock) fraud - Other types of equity investment fraud not mentioned above.

1.1.1.2 Debt investment fraud - A type of securities fraud in which the fraudulent investment vehicle is a bond or debt with a governmental body or corporation. Examples include promissory note fraud, prime bank note fraud, and bond fraud.

1.1.1.2.1 Promissory note fraud - A type of securities fraud that deals in the sale of promissory notes, a type of debt that is similar to a loan or IOU and is used by a company to raise money. Typically, an investor agrees to loan money to the company for a set period of time. In exchange, the company promises to pay the investor a fixed return on the investment, typically principal plus annual interest. While promissory notes can be legitimate investments, those that are marketed broadly to individual investors often turn out to be nothing more than worthless paper.

1.1.1.2.2 Prime bank note fraud - A type of securities fraud in which the instruments are marketed by promoters as debt or similar obligations purportedly issued by the "world prime banks." The fraudsters promise risk-free returns (typically 25% or more per year), but after selling the investments and perhaps making a few interest payments, they usually move the money offshore where investors can't retrieve it, then they disappear.

1.1.1.2.3 Bond fraud - Securities fraud dealing with fraudulent bonds. Examples might include bogus U.S. government securities, municipal bonds, corporate bonds, mortgage- and asset-backed securities, federal agency securities and foreign government bonds.

1.1.1.2.99 Other debt investment fraud - Other types of debt investment fraud not mentioned above.

1.1.1.99 Other securities fraud - Securities fraud not mentioned in the equity or debt investment fraud sections.

1.1.2 Commodities trading fraud - Fraud in connection with commodities transactions (such as transactions in foreign currency, agricultural products, energy products, and precious metals).

1.1.2.1 Forex (foreign exchange) fraud - This refers to any scheme used to defraud traders by convincing them that they can expect to gain a high profit by trading in the foreign exchange market. In many cases, the trader's money is never actually placed in the market through a legitimate dealer, but simply diverted into the bank account of the con artists.

1.1.2.2 Commodity pool fraud - Commodity pool operators are individuals or firms who raise funds and pool them together to trade commodities. In fraudulent commodity pools, scam artists misuse funds and solicit participants based on false claims of high profits. The operators may be unregistered and they may operate "Ponzi" schemes in which little or none of the victim's money is used for trading commodities.

1.1.2.3 Precious metals fraud - This is a type of commodities fraud in which individuals are promised easy profits from rising prices in precious metals, such as gold, silver, palladium, and platinum. Scam artists often tell victims that they only have to pay a small percentage of the total purchase price because a loan will be arranged to cover the balance. In reality, little or no money is actually used to purchase metals, but the scam artists may charge phony interest on the loan or false fees to "store" the metals.

1.1.2.99 Other commodities fraud - Other types of commodities fraud not mentioned above.

1.1.3 Other investment opportunities fraud - Other investment opportunities that are not securities or commodities.

1.1.3.1 Hollywood film scam - A scheme to defraud investors who believe they are investing in the production of a Hollywood movie. These are often operated out of boiler rooms where fraudsters cold call investors offering them "minimum risk" investments in movies that are soon to begin production with well-known actors. In reality, there is no movie and the fraudsters pocket the money.

1.1.3.2 Property/real estate scams - Fraudsters advertise or send out glossy brochures that invite prospective investors to attend a presentation where they will learn how to make money from investments in the property market. They are then pressured into joining for a fee or to buy "future" properties at a discount.

1.1.3.3 Rare objects scam - Investment fraud dealing in rare objects, like coins, artwork, or stamps.

1.2 Consumer Products and Services Fraud

This broad category covers all fraud related to the purchase of tangible goods and services. It also includes vacations and travel, house/apartment rentals, purchase of pets, concerts/performances, and other events or items the victim paid for but did not receive as promised. The category is further subdivided based on whether the fraud deals with a product, a service, or unauthorized billing. This broad category includes many fraud schemes, including bogus loans, worthless products, phony insurance, products paid and never received, unnecessary repairs, and many others.

1.2.1 Worthless or non-existent products - This category includes schemes that involve false or misleading information about products, goods, housing, or experiences (including vacations and concerts) that over exaggerate claims, turn out to be worth much less than anticipated, or are non-existent. In some forms of fraud involving worthless or non-existent items, consumers attempt to get their money back after cancelling their orders or returning the items to the fraudster, yet no refund is provided despite the fraudster's initial claims. Examples of worthless/nonexistent products include weight-loss scams, fake collectibles, and products that were purchased but never received.

1.2.1.1 Worthless products **-** A sub-category of "worthless or non-existent products," these are schemes that involve false or misleading information about products or goods that over exaggerate claims or turn out to be worth much less than anticipated.

1.2.1.1.1 Weight-loss products and health supplement scams - An example of a worthless product, fraudulent weight loss products and health supplements advertise unsubstantiated claims that consumers will be able to lose weight quickly or maintain their health without substantial changes to diet or exercise. They often involve the sale of dietary supplements as the means to lose weight.

1.2.1.1.2 Pharma discount scams - An example of worthless products, this refers to fraudulent fee-based pharmacy discount cards that purport to offer discounts on medications, but don't actually have any benefits.

1.2.1.1.3 Medical devices - An example of worthless products, this refers to fraudulent medical devices that advertise unsubstantiated claims and do not have proven benefits.

1.2.1.1.4 Cemetery plot scam - In this common worthless product scheme, an older victim doesn't want to burden their family with paying for a funeral or cemetery plot and so pays a large sum or an ongoing installment to reserve a spot. When the person dies, the plot is worth much less than what was paid.

1.2.1.1.5 Fake memorabilia - An example of worthless products, these scams refer to victims paying high dollar amounts for what they believe is valuable memorabilia, but turns out to be fake. Memorabilia includes collectible objects and cultural artifacts such as trading cards, coins, art, and film and sports paraphernalia.

1.2.1.1.6 Bogus software - In this example of a worthless product scam, the consumer is intentionally sold pirated or fake software that is falsely advertised as licensed software from a legitimate developer. The software turns out to be useless to the consumer.

1.2.1.1.7 Fake gemstones - In this example of a worthless product scam, the consumer is deliberately sold fake or poor quality gemstones that were advertised as valuable jewels.

1.2.1.1.99 Other - Other types of worthless products not mentioned above.

1.2.1.2 Paid never received - A sub-category of "worthless or non-existent products," these are schemes in which victims intentionally enter an agreement and pay for something that they never receive. A common example is online marketplace fraud where a victim sees an item advertised online and sends payment to the seller but the item is never delivered.

1.2.1.2.1 Online marketplace fraud - An example of paid never received, these scams involve items that are posted for sale or for rent by individual sellers on sites such as Craigslist, eBay, Etsy, and many others. Scam artists advertise items such as used vehicles, electronics, appliances, homemade items, collectibles, and also vacation, home, and apartment rentals, pets, event tickets, and other items. These items either do not exist, are never shipped, or are intentionally not refunded if the victim never received the item and then attempted to cancel the order.

1.2.1.2.99 Other - Other types of products or items that are paid for but never received.

1.2.1.99 Other - Other types of worthless of non-existent products not mentioned above.

1.2.2 Worthless, unnecessary, or non-existent services - Schemes in which victims intentionally enter an agreement for a service that turns out to involve false or misleading promotions or is not provided at all. Examples include phony insurance, credit repair schemes, and unnecessary or overpriced repairs.

1.2.2.1 Phony insurance - Schemes in which scammers falsely claim that they can provide consumers with insurance (health, auto, home, life, etc.), but provide no such service.

1.2.2.2 Immigration services/Notario fraud - “Notarios” or “Immigration Consultants” work throughout the United States and use false advertising and fraudulent contracts for services which cannot be provided. Notarios present themselves as qualified to help immigrants obtain lawful immigration status, and may charge considerable money for help that they never provide.

1.2.2.3 Invention fraud - In these schemes, firms solicit inventors with exaggerated promises to obtain valuable patents and make false claims about the potential market success of those inventions. These firms provide the inventor with basic market research for a large fee and, ultimately, obtain an overly narrow or useless patent that is worthless in the marketplace.

1.2.2.4 Fraud loss recovery - Also called "recovery room scams", this type of worthless services fraud preys on individuals who have already been victimized by fraud. The pitch typically used by recovery room telemarketers makes reference to the consumer's prior victimization, sympathetically warns him or her not to fall for telemarketing schemes again, and then falsely promises that they can help recover money lost in a previous scam for a fee or a donation to a specified charity.

1.2.2.5 Debt relief scam - Debt relief service scams solicit consumers by falsely promising to negotiate with their creditors to settle or otherwise reduce consumers' repayment obligations. These operations often charge consumers a large upfront fee, but then fail to help them settle or lower their debts to the promised level (if they provide any service at all).

1.2.2.5.1 Credit card debt relief scam - A sub-type of debt relief scam in which the type of debt is credit card debt. Often the scammers promise to negotiate with the consumer’s credit card company to secure lower interest rates, but for a large fee.

1.2.2.5.2 Mortgage relief scam - A sub-type of debt relief scam that deals with housing debt. Mortgage relief scammers falsely claim that, for a fee, they will negotiate with consumers’ mortgage lenders or servicers to obtain a loan modification or other relief to avoid delinquency or foreclosure. Some pretend to be affiliated with the government or government housing assistance programs, such as the Troubled Asset Relief Program (TARP) or the U.S. Department of Housing and Urban Development (HUD). Unfortunately, these operations often fail to obtain the relief they promise, and they sometimes fail to take even minimal steps to help consumers.

1.2.2.5.3 Student debt relief scam - A sub-type of debt relief scam in which the type of debt is student loans. Fraudsters falsely claim that, for a fee, they will negotiate with lenders to reduce the victim's student debt.

1.2.2.5.4 Medical debt relief scam - A sub-type of debt relief scam in which the type of debt is related to medical and healthcare expenses. Fraudsters falsely claim that, for a fee, they can help the victim reduce medical debt.

1.2.2.5.99 Other - Other types of debt relief scams not mentioned above.

1.2.2.6 Credit repair scam - Credit repair scams frequently target financially distressed consumers who are having credit problems. These operations entice consumers to purchase their services by falsely claiming that they will remove negative information from consumers' credit reports and/or improve their credit scores even if that information is accurate.

1.2.2.7 Fake credit lines and loans - These scams are often targeted at people with bad credit or in need of a loan. The scam may start as a legitimate appearing email or website offering online lending services, or a victim is informed they qualify for a loan over the telephone but first must pay money up front. In a common variant of this scam, an email encourages the recipient to click on a link to activate the new spending limit, but the link could lead to malware, requests for personal information, and a host of other problems. In another variant, a consumer responds to an ad or a phone call and is told that he/she is qualified for a loan or credit card, but must first pay an application fee or a security deposit in advance. The victim pays the money, but no loan or credit card is issued.

1.2.2.7.1 Fake loans - Often called “advance fee loans,” in this scam the consumer receives a phone call or is prompted to click on a link stating that the consumer qualifies for a loan and that the loan is not dependent on the consumer’s credit history. Before the loan is issued, a fee must be paid and the consumer may be asked to provide personal identifying information. Consumers may be told that the fee is for a security deposit, loan processing, or other paperwork, but the lender's fee structures are not properly disclosed and the loan is never provided.

1.2.2.7.2 Fake credit lines/credit cards - In these scams, consumers receive an enticing offer, either online or in the mail, to sign up for a new credit card. Applicants are told they must pay an upfront fee or deposit, but the card either never materializes, or is only accepted in certain retail outlets and catalogs selling outrageously overpriced goods. In a common online variant, applicants are encouraged to click on a link that will purportedly activate a new spending limit on their cards, but instead infects their computer with malware.

1.2.2.7.99 Other - Other types of fake credit and loans not mentioned above.

1.2.2.8 Fortune telling fraud - A type of scam in which a purported psychic or fortune teller convinces victims that a curse has been placed on them and their family. The fortune teller tells the victims that they can remove the curse for a fee.

1.2.2.9 Phishing websites/emails/calls - Phishing is a fraudulent attempt to acquire sensitive information by masquerading as a trustworthy entity. This is usually accomplished over the phone or via electronic communication in which the fraudster sends out bogus emails or tries to get potential victims to click on pop-ups, websites, or download software in an attempt to gather personal and financial information (credit card numbers, social security numbers, account numbers or passwords). Sometimes the scam involves tricking victims into entering their personal information online using official-looking websites that mimic websites managed by government agencies or banking institutions (spoofing).

1.2.2.9.1 Tech support scam - In this scheme, fraudsters call victims and claim to be computer techs associated with well-known companies. They say that they've detected viruses or other malware on the victims' computer to trick them into paying for unnecessary software (often that doesn't exist or is malware) or convince them to give the fraudsters remote access to the computer where they can gather more personal information on the victim.

1.2.2.9.2 Spoofing websites - In this scam, victims are prompted to enter their personal and/or financial information into websites that look official but turn out to be fake. Common examples of fake websites are online banking services, legal name change services, or government agency websites like the Social Security Administration, the Bureau/Department of Motor Vehicles, and city utilities departments.

1.2.2.9.99 Other - Other types of phishing scams not mentioned above.

1.2.2.10 Timeshare resale fraud - A timeshare involves joint ownership of a property that is usually located in popular vacation spots. These scams involve the fraudulent sale of timeshare properties, or promises to resell financially burdensome properties in cases where the victim is already an owner. The fraudsters promise that they have buyers lined up and collect fees from owners but do not deliver on their promises to sell their timeshares.

1.2.2.11 Adoption scam - Adoption fraud refers to any form of intentional misrepresentation or an illegal act in the area of adoption. Prospective birth families, adopting parents, and adoption professionals are all capable of adoption fraud. A prospective birth mother may promise her unborn child to multiple adopting families and accept money from each family while having no intention to make an adoption plan for her child. Another example would be an adoption agency requiring adopting families to pay exorbitant fees and then not providing the services promised.

1.2.2.12 Internet gambling fraud - This scam involves online games like poker, blackjack, roulette and other casino games that are just a front for channeling consumers' money. The victims never receive the money they have won, or the game is rigged so they are unable to win.

1.2.2.13 Fake buyers scam - A type of non-existent service in which the victim posts an item for sale, often on Craigslist or eBay, and is contacted by a fraudster. The buyer won't agree to meet in person and wants to pay by cashier's check, US Postal Service money order, Western Union, or an escrow service. The victim may send the item to the buyer but does not receive valid payment in return. A variation of this scheme occurs when fraudsters ask the victim to cash a (counterfeit) payment instrument that is for a larger sum than the selling price and then return any unintentional overpayment; or, when fraudsters indicate they are no longer willing to proceed with the purchase and request that the victim send a refund before the victim realizes the initial payment was invalid. In both instances, the victim is held liable by the bank where the counterfeit financial instrument was deposited and must repay any amount that was withdrawn in connection with the cashed counterfeit instrument.

1.2.2.14 Unnecessary or overpriced repairs, or repairs never performed - This type of worthless services fraud deals with unnecessary or overpriced repairs, or repairs never performed. Common examples are home and auto repair scams.

1.2.2.14.1 Auto repair fraud - Scams in which victims pay money for unnecessary or overpriced auto repairs, or pay for repairs that are not performed.

1.2.2.14.2 Home repair fraud - Scams in which victims pay money for unnecessary or overpriced home repairs, or pay for repairs that are not performed.

1.2.2.14.99 Other - Other types of unnecessary or overpriced repairs, or repairs never performed that are not mentioned above.

1.2.2.15 Travel booking scam - In this worthless services scam, a person claiming to be a travel agent or representative of a travel booking company deceives the victim into paying for a vacation or a vacation rental that either does not exist or is grossly misrepresented. Ultimately the victim does not receive the vacation package that were paid for.

1.2.2.16 Website hosting/design scam - In this scam, payment is collected from a consumer who is falsely promised that the scammer will design and/or host his or her website. Services are either never provided or not provided as promised.

1.2.2.17 Domain name scam - These scams involve fraudsters offering victims refusal on a domain name, saying that someone else is just about to buy it. The caller will often say that the individual has just minutes to accept the offer, and then try to pressure him or her into paying an excessive fee. In reality, no third party exists. Domain name scams can also come in the form of bogus domain name renewal notices.

1.2.2.99 Other - Other types of worthless or non-existent services in which victims enter the agreement intentionally.

1.2.3 Unauthorized billing for products or services - This sub-category of Consumer Products and Services Fraud pertains to both products and services, but in these types of scams, victims did not agree to pay the amount they were ultimately charged by the scam artist. In other words, victims are intentionally billed for products or services they did not order, or at a higher rate than was advertised.

1.2.3.1 Buyers' clubs - This refers to billing consumers without their consent for membership in a buyers' club. Buyer's clubs are memberships that allow consumers to purchase products or vacations (e.g., hotels, tours, cruises) at a discounted price. Telemarketers may offer consumers a free trial membership in a buyers' club as a "thank you" for their purchase of some unrelated product or a vacation they paid full price for. Sometimes the membership is offered as a negative option ("opt out"), which means that the credit card that the consumer used to make the initial purchase is automatically charged for the price of the membership unless the membership is cancelled by the end of the free trial period.

1.2.3.2 Unauthorized billing: Internet services - In this scam, the victim receives an unauthorized bill for Internet services such as Internet access, website hosting or web development.

1.2.3.2.1 Online yellow pages - Unauthorized billing for online yellow pages services.

1.2.3.2.99 Other - Unauthorized billing for other internet services not mentioned above.

1.2.3.3 Unauthorized billing: Phone services - Unauthorized billing for telephone (landline or cellular) services.

1.2.3.3.1 Cramming - A type of unauthorized phone billing, "cramming" is the practice of placing unauthorized, misleading, or deceptive charges on a victim's standard mobile or landline telephone bill.

1.2.3.3.2 Slamming - A type of unauthorized phone billing, "slamming" is the illegal practice of switching a consumer's traditional wireline telephone company for local, local toll, or long distance service without permission.

1.2.3.3.99 Other - Other types of unauthorized phone billing not mentioned above.

1.2.3.4 Unauthorized billing: Magazines - Unauthorized billing for magazine subscriptions.

1.2.3.5 Unauthorized billing: Credit monitoring services - Unauthorized billing for credit report or credit monitoring services.

1.2.3.99 Other unauthorized billing fraud - Other types of unauthorized billing for products or services not mentioned above.

1.2.99 Other consumer products and services fraud - Other consumer products and services fraud not described above.

1.3 Employment Fraud

In this broad category of fraud schemes, the expected benefit is employment or training to develop a profitable business. Fraudsters advertise work opportunities that require few skills or qualifications, but claim to provide above average financial rewards. The fraudsters secure money through upfront fees or by asking consumers to pay for materials to enable them to become involved, but in reality there is no paid work or the business venture is not nearly as profitable as the scam artist had guaranteed. A variation of this scheme occurs when fraudsters pay the victim with a counterfeit check or money order. The fraudsters then ask the victim to deposit the counterfeit instrument and return to the fraudster any unintentional overpayment. The victim is held liable by the bank where the counterfeit financial instrument was cashed and must repay to the bank any amounts withdrawn in connection with the cashed counterfeit instrument. This broad category includes the sub-categories of: business opportunities fraud, work-at-home scams, government job placement scams, and other employment scams. Common examples in this broad category include multi-level marketing schemes, mystery shopper scams, and nanny scams.

1.3.1 Business opportunities fraud - This broad sub-type of employment fraud includes business opportunities (or "biz opps") where victims are promised the tools, training, or equipment needed to create their own profitable business or way to generate income, such as day trading, selling products, or leasing vending/ATM machines. This often involves the sale or lease of a product, service or equipment that will enable the purchaser/licensee to begin a business, or the promise to coach/train the consumer to be successful in a business venture. In the end, the companies offering these services fail to follow through on their promises, or the profits are much less than what the company led the participant to believe.

1.3.1.1 Multi-level marketing scheme - Multi-level marketing (MLM) is a marketing strategy in which the sales force is compensated not only for sales they generate, but also for the sales of the other salespeople that they recruit. These schemes can be fraudulent if the company promises members that they can make a certain amount of money or that they will offer assistance and then don't deliver. MLMs can also operate as illegal pyramid schemes in which profit is earned not by the sale of the product, but by the sale of new distributorships. The emphasis on recruitment rather than the product eventually leads to a point where the supply of potential investors is exhausted and the pyramid collapses.

1.3.1.2 Vending machines/ATM leasing scam - Scams in which fraudsters make unsubstantiated claims to business opportunity buyers in connection with the sale or lease of vending machines and ATM machines.

1.3.1.3 House flipping courses - Fraudsters offer seminars with supposed insider tips about how to make a profit “flipping houses,” or buying properties at depressed rates, fixing them up, and selling them quickly for a large profit. Fraudsters often entice victims with a free seminar, but subsequent seminars can cost exorbitant amounts of money despite offering nothing substantive.

1.3.1.4 Business coaching scam - In this scam, consumers are contacted over the phone or respond to online advertisements for business coaching services. The companies promise to provide them with training and tools to launch a successful business online. These services are never delivered as promised and the victim is often charged high fees.

1.3.1.99 Other - Other types of business opportunity scams not mentioned above.

1.3.2 Work-at-home scam - Fraudsters advertise work opportunities that require few skills or qualifications, but claim to provide above average financial rewards. The fraudsters secure upfront fees to enable the victim to become involved, but in reality there is no paid work. Work-from-home scams differ from business opportunity scams in that victims believe they are being hired to do a specific job for a specific employer, rather than believing they are gaining tools to begin their own businesses. Common work-at-home scams include stuffing envelopes, mystery shopping, home assembly kits. In a common variant of this scheme, fraudsters overpay the victim with a counterfeit check or counterfeit money order. They then ask the victim to immediately return any unintentional overpayment to the fraudster after the check is cashed. The victim is then held liable by the bank and must repay any amounts withdrawn in connection with the cashed counterfeit instrument.

1.3.2.1 Home assembly - In this scam, victims are promised unrealistic earnings for assembling crafts and other products that are supposedly going to be resold to other customers. Participants are required to pay the promoter for all materials and kits to be assembled, but when the product is assembled, it often does not pass the company’s “inspection” process. Ultimately, victims pay the company more for kits and instructions than they receive for assembling products.

1.3.2.2 Envelope stuffing - This is a common work-at-home scam in which victims purchase all of the supplies (envelopes, stamps or stamp meter, etc.) and may have to stuff thousands of envelopes just to break even.

1.3.2.3 Mystery shopper - Fraudsters create websites where an individual can register to become a mystery shopper, or they solicit potential victims over the phone or by email. First victims have to pay a fee for information about a certification program, a directory of mystery shopping companies, or a guarantee of a mystery shopping job. In one variation of the scam, a victim is asked to evaluate the effectiveness of a money transfer service. The victim is led to believe that the purpose of the transfer is to evaluate the experience, but no one collects the evaluation because it is just a ruse to get the victim’s money. First the victim is mailed a counterfeit check, told to deposit it into a personal bank account, and then to withdraw the amount in cash. The victim is then instructed to transfer those funds using the money transfer service specified. The original check bounces while the victim’s real funds are sent to the scammer or the scammer’s criminal affiliates.

1.3.2.4 Reshipping - In these scams, so-called large multi-national companies recruit people to re-ship products all over the world. A legitimate company would never operate in this fashion, so "employees" are likely participating in an illegal theft or counterfeit enterprise.

1.3.2.99 Other - Other types of work-at-home scams not mentioned above.

1.3.3 Government job placement scam - Scams in which fraudsters collect payment from victims to purportedly help them secure government jobs, when no jobs exist.

1.3.4 Other employment scam - Other employment scams not mentioned above. As with all employment scams, the expected benefit of the fraud is a job.

1.3.4.1 Nanny scam - In a typical nanny scam, a nanny who has a posting on an online site is contacted by a scammer who wants to hire him/her without having an interview first. The scammer will send a forged money order or some other form of payment to the nanny as advance payment to secure him/her for the job or for purchasing items needed for the job. When the money arrives, it is for much more than expected and the scammer sends instructions about sending the excess money to a third party, which is actually going right back to the fraudster or his/her criminal affiliates. When the initial deposit from the scammer doesn't clear, the nanny is left with the out-of-pocket cost of the excess amount sent back to the fraudster.

1.3.4.2 Modeling scam - In this scam, a “recruiter” stops an individual in a public place, often at the mall, and says that he/she could be a model. The fraudster organizes a modeling job “interview,” which is really a high-pressure sales pitch for modeling or acting classes, screen tests, or photo shoots that can range in price from several hundred to several thousand dollars.

1.4 Prize and Grant Fraud

The hallmark of this category of fraud is that victims are led to believe they will receive winnings in the form of a prize, lottery, grant, or windfall of money, provided that they first purchase certain products or make advance payments to cover fictitious fees and taxes. This type of fraud includes prize promotions/sweepstakes scams, lottery scams, government grant scams, inheritance scams, and Nigerian letter scams, among others.

1.4.1 Prize promotion/sweepstakes scam - Fraudsters send out letters, use email, or call potential victims telling them they have won a prize or are entitled to a financial reward, but they need to call an expensive 900 number or pay a small 'administrative' or shipping and handling fee to obtain their winnings. In some cases the scam artist claims the victim won a “sweepstakes” even though the consumer did not enter a sweepstakes contest. In other cases, the scam artist sends out a sweepstakes promotion that requires an entry fee to participate, but no legitimate sweepstakes would require payment to enter.

1.4.1.1 Free product - A type of prize promotion scam in which the supposed prize is a product, ranging from small trinkets to brand new cars.

1.4.1.2 Free vacation - A type of prize promotion scam in which the supposed prize is a vacation.

1.4.1.3 Cash prize - A type of prize promotion scam in which the supposed prize is cash.

1.4.1.4 Sweepstakes scam - A legitimate sweepstakes is an advertising or promotional device by which money or prizes are awarded to participating consumers by chance, with no purchase or “entry fee” required to win. While many prize promotion scams are advertised by fraudsters as a “sweepstakes”, a true sweepstake scam requires that victims pay a bogus entry free in order to win. Fraudsters send fake sweepstakes promotions to unsuspecting consumers describing valuable prizes that they can win after sending back the completed form plus a fee (or after making a purchase) to enter. Consumers often lose all the money they send, or, if a product is ever received, it is usually of poor quality.

1.4.1.99 Other - Other types of prize promotions scams not mentioned above.

1.4.2 Bogus lottery scam - Victims are told they have won a lottery and they need to pay an 'administrative' fee or tax to receive the winnings. This type of fraud is perpetrated via mail, e-mail, and telephone. Sometimes the victims are also asked to contact another agent by telephone in order to proceed.

1.4.2.1 Foreign lottery scam - In this bogus lottery scam, victims are told they won money in a foreign lottery but are required to pay money upfront to cover the taxes, pay customs officials, or to cover legal and administrative costs. These lottery solicitations violate U.S. law, which prohibits the cross-border sale or purchase of lottery tickets by phone or mail.

1.4.2.99 Other - Other types of bogus lotteries that claim to be domestic or that are not listed above.

1.4.3 Nigerian letter fraud - Nigerian letter frauds are a variation of an advance fee scheme in which a letter or email from Nigeria offers the recipient the “opportunity” to share in a percentage of millions of dollars that the author, a self-proclaimed government official, is trying to transfer out of Nigeria. The victim is encouraged to send personal and banking information to the “official” in Nigeria to facilitate the transfer of money. Though this type of fraud has many elements, it is categorized in "Prize and Grant Fraud" because the key element of the fraud is the promise of a windfall of money.

1.4.4 Government grant scam - These scams start with an ad that claims an individual qualifies to receive a “free grant” to pay for education costs, home repairs, home business expenses, or unpaid bills. Other times, it’s a phone call supposedly from a “government” agency or some other organization with an official sounding name. The fraudsters claim that the application for a grant is guaranteed to be accepted, and the individual will never have to pay the money back. They then ask for an administration fee to cover the cost of the application, or they ask for bank account information to deposit the grant money.

1.4.5 Inheritance scam - Fraudsters pose as “estate locators” contacting the victim via email. In their correspondence, they will indicate an unclaimed inheritance is waiting for the victim. The fraudsters make money by asserting they’ve put together an estate report that includes information on where the inheritances are located and how they can be claimed. For a relatively small fee, the victim can receive the report, which in reality does not exist.

1.4.6 IRS tax refund opportunity - In these scams, fraudsters call consumers claiming to be from the IRS. They tell victims that they are eligible for a tax refund and ask for sensitive account information about where to deposit the refund. Though this type of fraud uses phishing tactics to get information from consumers, it is categorized in "Prize and Grant Fraud" because victims are promised a windfall of money in tax refunds.

1.4.99 Other prize and grant fraud - Other types of prize and grant fraud not mentioned above.

1.5 Phantom Debt Collection Fraud

This category of fraud refers to fake debt collectors who deceive and possibly threaten individuals to convince them to pay debts they don't owe. Sometimes the collectors use fictitious names that imply they are affiliated with a law firm, a prominent lending institution, or the government. They may threaten the victim with serious repercussions, like being sued, being arrested, having their bank account closed, their wages garnished, or being forced to appear in court if they do not pay back their debts. This broad category is further subdivided into government debt collection scams, lender debt collection scams, and business debt collection scams based on the type of false debt.

1.5.1 Government debt collections scam - A sub-type of "Phantom Debt Collection Fraud" in which fraudsters impersonate government officials to convince individuals to pay back debt they don't owe. Common examples include court impersonation scams and IRS back taxes owed schemes.

1.5.1.1 Court impersonation scam - Scammers impersonate court and police officials (possibly using caller ID technology) and call people with false claims that they have missed a court date, a fine payment, or jury duty. The fraudsters claim that an arrest warrant will be issued unless the victim pays a fine.

1.5.1.2 IRS back taxes scheme - Scammers impersonate IRS officials and contact individuals claiming that they owe back taxes or fees to the IRS.

1.5.1.99 Other - Other types of government debt collection scams not mentioned above.

1.5.2 Lender debt collection scams - A sub-type of "Phantom Debt Collection Fraud" in which fraudsters impersonate well-known lending institutions to convince individuals to pay back debt they don't owe. A common example is an obituary scam.

1.5.2.1 Obituary scam - In this scheme, scammers review the obituary sections of small-town newspapers looking for a recent death leaving behind a widow. They will then call the widow and tell her that her recently deceased husband actually had thousands of dollars in unpaid debt that is now due. The fraudsters will often threaten financial ruin and eviction unless the debt is paid very rapidly.

1.5.2.2 Loan debt scam - In this scam, victims are contacted by scam artists claiming that they have unpaid debt associated with a personal loan that was provided sometime in the past. In some cases the victims already paid back the supposed loan, and in other cases the victims were never loaned money to begin with, like in advance fee loan scams.

1.5.2.99 Other - Other types of lender debt collection scams not mentioned above.

1.5.3 Business debt collection scams - A sub-type of "Phantom Debt Collection Fraud" in which fraudsters impersonate well-known businesses to convince individuals to pay back debt they don't owe.

For example, this could include fake health and medical debt supposedly owed to a hospital or insurance agency.

1.5.3.1 Fake health and medical debt - A type of phantom debt scam in which an individual is contacted by scammers claiming they are from a hospital or insurance agency demanding payment for fake health and medical debt.

1.5.3.99 Other - Other types of business debt collection scams not mentioned above.

1.5.99 Other phantom debt frauds - Other types of phantom debt scams not mentioned above.

1.6 Charity Fraud

This category of fraud involves scam artists collecting money by posing as a genuine charity. There is no expected benefit or product/service resulting from the transaction. Instead, the expected outcome from the perspective of the victim is organized charitable giving. This category is sub-divided into bogus charitable organizations and crowdfunding for bogus causes depending on whether the fraudulent entity is supposedly a non-profit organization or an online crowdfunding account where individuals can donate money.

1.6.1 Bogus charitable organization - A sub-type of charity fraud in which the fraudsters collect donations by pretending to be genuine non-profit organizations representing a variety of causes, from natural disaster relief to children's issues.

1.6.1.1 Bogus natural disaster-related charity - A type of bogus charitable organization in which the fraudsters claim to be a natural disaster relief charity.

1.6.1.2 Bogus disease-related charity - A type of bogus charitable organization in which the fraudsters claim to be a charity that works to find cures for diseases or to support those who are ill.

1.6.1.3 Bogus law enforcement charity - A type of bogus charitable organization in which the fraudsters claim to be a charity that benefits law enforcement.

1.6.1.4 Bogus veteran charity - A type of bogus charitable organization in which the fraudsters claim to be a charity that benefits war veterans.

1.6.1.5 Bogus church/religious group charity - A type of bogus charitable organization in which the fraudsters claim to be a church-related charity.

1.6.1.6 Bogus animal shelter - A type of bogus charitable organization in which the fraudsters claim to be an animal shelter or charity that helps animals in some way.

1.6.1.7 Bogus alumni charitable giving - A type of bogus charitable organization in which the fraudsters claim to be collecting donations on behalf of the victim's alumni association.

1.6.1.8 Bogus children's charity - A type of bogus charitable organization in which the fraudsters claim to be a charity that addresses children's issues, like sponsoring children overseas.

1.6.1.9 Bogus political group - A type of bogus charitable organization in which the fraudsters claim to be collecting donations on behalf of a political organization.

1.6.1.10 Bogus youth organization - A type of bogus fundraiser in which fraudsters misrepresent themselves as part of an association or group raising money for children's educational expenses or class trips (i.e., claiming to be students).

1.6.1.99 Other - Other types of bogus charities not mentioned above.

1.6.2 Crowdfunding for bogus personal cause - A sub-type of charity fraud in which the fraudster sets up a personal crowdfunding account and collects donations by pretending to be a victim. Common examples include creating false stories of medical debt or creating accounts that supposedly collect money for victims of natural disasters or national tragedies.

1.6.2.1 Fake personal medical expenses - A type of bogus crowdfunding in which a fraudster fabricates an illness to raise money for supposed medical debt.

1.6.2.2 False identity as natural disaster or national tragedy survivor - A type of bogus crowdfunding in which a fraudster pretends to be a survivor of a natural disaster or national tragedy to raise money.

1.6.2.99 Other - Other types of crowdfunding for bogus personal causes not mentioned above.

1.6.99 Other charity fraud - Other types of charity fraud not mentioned above.

1.7 Relationship and Trust Fraud

In these schemes, the fraudster exploits a personal relationship with the victim and there is no expectation of a product or service from the interaction. Instead, the expected outcome from the perspective of the victim is the fostering of a personal relationship. The fraudster can either exploit a pre-existing personal relationship by pretending to be a friend or relative (imposter scams) or can create a new personal relationship with the intention to exploit the victim at a later date (romance scam). In both of these examples, the fraudster relies on exploiting the belief that he or she is engaged in a supposed personal and genuine relationship with the perpetrator.

1.7.1 Romance scam/Sweetheart scam - A type of "Relationship and Trust Fraud," in these scams, victims are contacted in-person or online by someone who appears interested in them. In many cases, the fraudster sets up a fake online profile using a photo found on the internet ("catfishing"). Over the course of weeks or months, they develop what the victim believes to be a true romantic relationship. Eventually, the perpetrator will ask for money for a variety of reasons, which may include wanting to visit the victim but being unable to afford the flight, needing to clear a debt, or wanting to help out a dear relative. The money is often requested in un-traceable ways, like a money order or a prepaid card.

1.7.2 Friends or relatives imposter scams - This is a type of "Relationship and Trust Fraud" in which fraudsters pretend to be a victim's friend or relative and ask for money in an unexpected call or email. This is often accomplished by hacking into Facebook or other social media accounts and sending messages to the victims. This category also includes grandparent scams.

1.7.2.1 <u>Grandparent scam</u> - This is a common example of friends/relatives imposter scam. In these schemes, older adults receive a call from someone claiming to be their grandchild, niece, nephew, son, or daughter. The caller says there is an emergency and asks the elderly victim to send money immediately. The "grandchild" often claims to be out of the country and asks the older victim not to tell anyone because of embarrassment or fear of getting into trouble with other relatives.

1.7.2.99 <u>Other</u> - Other types of friends or relatives imposter scams not mentioned above.

1.7.99 Other relationship and trust fraud - Other types of relationship and trust fraud not mentioned above.

(2) Fraud against an organization

This broad category includes all fraud that is committed against an organization rather than an individual. The "victims" include government agencies, programs and regulations, society, and public, private, and nonprofit organizations and businesses.

2.1 Fraud against government agencies, programs, regulations, and society

In these schemes, it is not just the organization, but society as a whole, that must bear the direct and indirect cost of fraud.

2.1.1 Government Programs

Examples of fraud against government programs include welfare fraud, disability fraud, Medicare and Medicaid fraud, among others.

2.1.2 Government Regulations

Examples of fraud against government regulations include immigration fraud, voting fraud, tax fraud, and stamp fraud, among others.

2.1.3 Other

Examples of other frauds that affect society as a whole are insider trading and environmental fraud.

2.2 Fraud against an organization or business (public, private, or nonprofit)

This broad category includes all fraud committed against an organization or business. This includes public, private, and nonprofit agencies. This category is further divided into occupational fraud, which means the perpetrator was internal to the organization (an employee), and fraud committed by an external perpetrator.

2.2.1 Occupational Fraud (committed by internal perpetrator)

Following the Association of Certified Fraud Examiners' (ACFE) typology[7], examples of occupational fraud include corruption, asset misappropriation, and financial statement fraud.

2.2.2 Fraud committed by external perpetrator

Examples of fraud committed by a perpetrator external to the organization include insurance fraud, bank fraud, and fraudulent suppliers.

[7] http://www.acfe.com/fraud-tree.aspx

Attribute tags

Incident Tags

General Incident Tags

AF - Affinity fraud: an attempt to defraud members of a particular religious, ethnic, professional, age, or social group by members of these groups or persons claiming to provide assistance to these groups. This tag is particularly relevant for consumer investment fraud.

PS - Pyramid scheme: any fraudulent scheme in which participants make money solely by recruiting new participants into the program. The hallmark of these schemes is the promise of sky-high returns in a short period of time for doing nothing other than handing over money and getting others to do the same. This tag can be applied to types of business opportunity fraud (e.g., some multi-level marketing schemes) to indicate that the fraudulent activity involved operating as an illegal pyramid scheme.

PZ - Ponzi scheme: an investment fraud scheme in which the con artist (or “Ponzi”) pays “dividends” to initial investors using the funds of subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of “dividends.” This tag can be applied to various types of consumer investment fraud to indicate that they operated as Ponzi schemes.

IG - Impersonating a government official: any fraudulent scheme in which the perpetrator impersonates a government official to carry out the scheme. This tag could be applied to several fraud types, including certain types of prize and grant fraud and phantom debt fraud.

PD - Pump & dump scheme: an investment fraud scheme in which promoters hype up investor sentiment in a little-known or unknown stock. New investors rush in, thus "pumping" up its price. Once shares are inflated, insiders then "dump" their shares at a huge profit and leave investors with large losses. This tag can be applied to some types of investment fraud, including some securities fraud (e.g., penny stock fraud) and some commodities fraud types.

HM - Health or medical related fraud: any fraud that deals with a health or medical-related issue. This information is supplied as a tag because it applies to many different examples in multiple broad fraud categories. For example, this tag could be added to instances of worthless products (e.g., pharma discounts and medical devices), worthless services (e.g., phony insurance), and phantom debt collection (e.g., phony health and medical debt), among others.

CS - Continuity scam (aka negative option [or opt out] scam): any fraud that induces consumers to provide a credit card number and uses deceptive practices to obtain the appearance of the consumer's agreement to charge an automatic recurring fee. This tag can be applied to many different types of unauthorized billing fraud.

OV - Overpayment fraud: this fraud is often executed using a counterfeit check. Victims are provided a counterfeit check and are asked to refund any unintentional overpayment back to the scam artist, or to send a portion of the amount to cover the taxes and fees associated with a supposed prize or lottery winnings. As instructed, victims deposit the counterfeit instrument and then withdraw real funds from their personal accounts to send to the scammer before the original check clears. The original check is subsequently returned as a counterfeit but the refund has already been sent. These real funds are lost and the victims must cover the fees associated with depositing counterfeit checks.

CP - Counterfeit payment instrument: any fraud in which the victim is given a counterfeit payment instrument as their supposed prize/lottery winnings, or payment for an item, a service, or a job that the victim was asked to perform for the scam artist. Counterfeit payment instruments come in many forms: cashier's checks, money orders, and corporate and personal checks. Victims are responsible to cover any fees and charges associated with depositing the counterfeit instrument.

Method of Advertising the Fraud: How was the fraud advertised or promoted to victims? Where did the victim first learn about it?

Ad:IE - Internet, email

Ad:TX - Text, direct message

Ad:DM - Direct mail

Ad:TVR - TV or radio

Ad:T - Telemarketing

Ad:P - In person

Purchase Setting: In what setting was the fraudulent purchase made?

PS:I - Computer via Internet

PS:M - Mail

PS:T - Telephone

PS:S - Store (brick and mortar)

PS:P - Person to person

Method of Money Transfer: How did the money move from the possession of the victim to the possession of the perpetrator?

MT:CC - Credit card

MT:DC - Debit/ATM card

MT:C - Cash

MT:PC - Personal check

MT:M - Mobile/online payment application (e.g., Apple Pay, Square, Venmo, Google Wallet)

MT:MO - Money order

MT:W - Wire funds (e.g., Western Union, Money Gram, or bank)

MT:T - Telephone account

MT:PP - Prepaid card (e.g., Green Dot, Vanilla card, Bluebird, Walmart MoneyCard)

MT:B - Bitcoin

Dollar loss categories: Dollar loss categories indicate how much money the victim lost in the fraudulent transaction (if known).

Duration of incident: If the victim lost money over a period of time involving a series of transactions, duration categories indicate how long the fraudulent incident lasted.

Victim Tags

MV - Male Victim: The victim of the fraud was male.

FV - Female Victim: The victim of the fraud was female.

EV - Elder Victim: The victim of the fraud was age 65 or over. This tag identifies a type of fraud with particular policy relevance.

VV - Veteran Victim: The victim of the fraud was a veteran. This tag identifies a type of fraud with high policy relevance.

CIV - Cognitively Impaired Victim: The victim of the fraud was cognitively impaired. This tag identifies a type of fraud with high policy relevance.

RV - Repeat Victim: The individual has been victimized in the past by the same or a different type of fraud.

RA - The victim reported the fraud to authorities.

Perpetrator Tags

MP - Male Perpetrator: The perpetrator of the fraud was male.

FP - Female Perpetrator: The perpetrator of the fraud was female.

IP - Intimate Partner Perpetrator: The perpetrator of the fraud was an intimate partner of the victim, including boyfriend/girlfriend, former and current spouse.

FP - Family member Perpetrator: The perpetrator of the fraud was a family member of the victim, such as a child, parent, spouse, or other relative.

CP - Caregiver Perpetrator: The perpetrator of the fraud was the victim's caregiver.

Sources consulted for many of the definitions:

Federal Bureau of Investigation, *Common Fraud Schemes*
FINRA, *Investor Alerts*
Federal Trade Commission, *Scam Alerts*
Securities and Exchange Commission, *Investor Alerts*

Taxonomy of fraud

Attribute Tags

Incident Tags			Victim Tags	Perpetrator Tags
General Incident Tags	**Purchase Setting**	**Dollar loss categories**	MV - Male victim	MP - Male perp
AF - Affinity fraud	PS:I - Computer via the Internet	**Duration of incident**	FV - Female victim	FP - Female perp
PS - Pyramid scheme	PS:M - Mail		EV - Elder victim (age 65+)	IP - Intimate partner perp
PZ - Ponzi scheme	PS:T - Telephone		VV - Veteran victim	FP - Family member perp
IG - Impersonated Government official	PS:S - Store		CIV - Cognitively impaired victim	CP - Caregiver perp
PD - Pump & dump scheme	PS:P - Person to person		RV - Repeat victim	
HM - Health or medical related fraud	**Method of Money Transfer**		RA - Victim reported fraud to authorities	
CS - Continuity scam	MT:CC - Credit card			
OV - Overpayment fraud	MT:DC - Debit/ATM card			
CP - Counterfeit payment instrument	MT:C - Cash			
Method of Advertising the Fraud	MP:PC - Personal check			
Ad:IE - Internet, email	MT:M - Mobile/online payment application			
Ad:TX - Text/direct message	MT:MO - Money order			
Ad:DM - Direct mail	MT:W - Wire funds			
Ad:TVR - TV or radio	MT:T - Telephone account			
Ad:T - Telemarketing	MT:PP - Prepaid Card			
Ad:P - In person	MT:B - Bitcoin			

	Level 1		Level 2		Level 3		Level 4		Level 5
Category	*Who is the target?*		*What is the fraud category?*		*What is the type of fraud?*		*Some common examples or more specific sub-types*		*Some common examples or more specific sub-types*
1	**Individual Financial Fraud** (Fraud against an **individual)**	1.1	**Consumer Investment Fraud** *(expected investment returns)*	1.1.1	Securities fraud	1.1.1.1	Equity investment fraud	1.1.1.1.1	Penny stock fraud
								1.1.1.1.2	Pre-IPO scam
								1.1.1.1.3	High-yield investment program fraud
								1.1.1.1.4	REIT (Real Estate Investment Trust) fraud
								1.1.1.1.5	Oil & gas exploration scam
								1.1.1.1.6	Alternative energy company scam
								1.1.1.1.99	Other equity (stock) fraud
						1.1.1.2	Debt investment fraud	1.1.1.2.1	Promissory note fraud
								1.1.1.2.2	Prime bank note fraud
								1.1.1.2.3	Bond fraud
								1.1.1.2.99	Other debt investment fraud
						1.1.1.99	Other securities fraud		
				1.1.2	Commodities trading fraud	1.1.2.1	Forex (foreign exchange) fraud		
						1.1.2.2	Commodity pool fraud		
						1.1.2.3	Precious metals fraud		
						1.1.2.99	Other commodities fraud		
				1.1.3	Other investment opportunities fraud	1.1.3.1	Hollywood film scam		
						1.1.3.2	Property/real estate scam		
						1.1.3.3	Rare objects scam		
		1.2	**Consumer Products and Services Fraud** *(expected products, services, and other items)*	1.2.1	Worthless or non-existent products (intentionally entered agreement)	1.2.1.1	Worthless products	1.2.1.1.1	Weight-loss products and health supplement scams
								1.2.1.1.2	Pharma discount scam
								1.2.1.1.3	Medical devices
								1.2.1.1.4	Cemetery plot scam
								1.2.1.1.5	Fake memorabilia
								1.2.1.1.6	Bogus software
								1.2.1.1.7	Fake gemstones
								1.2.1.1.99	Other
						1.2.1.2	Paid never received	1.2.1.2.1	Online marketplace fraud
								1.2.1.2.99	Other
						1.2.1.99	Other		
				1.2.2	Worthless, unnecessary, or non-existent services (intentionally entered agreement)	1.2.2.1	Phony insurance		
						1.2.2.2	Immigration services/Notario fraud		
						1.2.2.3	Invention fraud		
						1.2.2.4	Fraud loss recovery		
						1.2.2.5	Debt relief scam	1.2.2.5.1	Credit card debt relief scam
								1.2.2.5.2	Mortgage relief scam
								1.2.2.5.3	Student debt relief scam
								1.2.2.5.4	Medical debt relief scam
								1.2.2.5.99	Other
						1.2.2.6	Credit repair scam		
						1.2.2.7	Fake credit lines and loans	1.2.2.7.1	Fake loans
								1.2.2.7.2	Fake credit lines/credit cards
								1.2.2.7.99	Other
						1.2.2.8	Fortune telling fraud		
						1.2.2.9	Phishing websites/emails/calls	1.2.2.9.1	Tech support scam
								1.2.2.9.2	Spoofing websites
								1.2.2.9.99	Other
						1.2.2.10	Timeshare resale fraud		
						1.2.2.11	Adoption scam		
						1.2.2.12	Internet gambling fraud		
						1.2.2.13	Fake buyers scam		
						1.2.2.14	Unnecessary or overpriced repairs, or repairs never performed	1.2.2.14.1	Auto repair fraud
								1.2.2.14.2	Home repair fraud
								1.2.2.14.99	Other
						1.2.2.15	Travel booking scam		
						1.2.2.16	Website hosting/design scam		
						1.2.2.17	Domain name scam		
						1.2.2.99	Other		
				1.2.3	Unauthorized billing for products or services	1.2.3.1	Buyer's clubs		
						1.2.3.2	Unauthorized billing - Internet services	1.2.3.2.1	Online yellow pages
								1.2.3.2.99	Other
						1.2.3.3	Unauthorized billing - Phone services	1.2.3.3.1	Cramming
								1.2.3.3.2	Slamming
								1.2.3.3.99	Other
						1.2.3.4	Unauthorized billing - Magazines		
						1.2.3.5	Unauthorized billing - Credit monitoring services		
						1.2.3.99	Other		
				1.2.99	Other consumer products & services				

Level 1	Level 2	Level 3	Level 4	Level 5
	1.3 **Employment Fraud** *(expected employment)*	1.3.1 Business opportunities fraud	1.3.1.1 Multi-level marketing scheme	
			1.3.1.2 Vending machines/ATM leasing scam	
			1.3.1.3 House flipping courses	
			1.3.1.4 Business coaching scam	
			1.3.1.99 Other	
		1.3.2 Work-at-home scam	1.3.2.1 Home assembly	
			1.3.2.2 Envelope stuffing	
			1.3.2.3 Mystery Shopper	
			1.3.2.4 Reshipping	
			1.3.2.99 Other	
		1.3.3 Government job placement scam		
		1.3.4 Other employment scam	1.3.4.1 Nanny scam	
			1.3.4.2 Modeling fraud	
	1.4 **Prize and Grant Fraud** *(expected winnings in the form of a prize, lottery, grant, or other windfall of money)*	1.4.1 Prize promotion/Sweepstakes scam	1.4.1.1 Free product	
			1.4.1.2 Free vacation	
			1.4.1.3 Cash Prize	
			1.4.1.4 Sweepstakes scam	
			1.4.1.99 Other	
		1.4.2 Bogus lottery scam	1.4.2.1 Foreign lottery scam	
			1.4.2.99 Other	
		1.4.3 Nigerian letter fraud		
		1.4.4 Government grant scam		
		1.4.5 Inheritance scam		
		1.4.6 IRS tax refund opportunity		
		1.4.99 Other prize & grant fraud		
	1.5 **Phantom Debt Collection Fraud** *(expected benefit is avoiding the consequences of failing to pay debts that the victim did not previously know were owed [and that turn out to be fake])*	1.5.1 Government debt collections scam	1.5.1.1 Court impersonation scam	
			1.5.1.2 IRS back taxes scheme	
			1.5.1.99 Other	
		1.5.2 Lender debt collection scam	1.5.2.1 Obituary scam	
			1.5.2.2 Loan debt scam	
			1.5.2.99 Other	
		1.5.3 Business debt collection scam	1.5.3.1 Fake health and medical debt	
			1.5.3.99 Other	
		1.5.99 Other phantom debt fraud		
	1.6 **Charity Fraud** *(expected outcome is charitable giving)*	1.6.1 Bogus charitable organization	1.6.1.1 Bogus natural disaster-related charity	
			1.6.1.2 Bogus disease-related charity	
			1.6.1.3 Bogus law enforcement charity	
			1.6.1.4 Bogus veteran charity	
			1.6.1.5 Bogus church/religious group charity	
			1.6.1.6 Bogus animal shelter	
			1.6.1.7 Bogus alumni charitable giving	
			1.6.1.8 Bogus children's charity	
			1.6.1.9 Bogus political group	
			1.6.1.10 Bogus youth organization	
			1.6.1.99 Other	
		1.6.2 Crowdfunding for bogus cause	1.6.2.1 Fake personal medical expenses	
			1.6.2.2 False identity as natural disaster or national tragedy survivor	
			1.6.2.99 Other	
		1.6.99 Other charity fraud		
	1.7 **Relationship & Trust Fraud** *(expected outcome is fostering a relationship)*	1.7.1 Romance scam/Sweetheart scam		
		1.7.2 Friends or relatives imposter scam	1.7.2.1 Grandparent scam	
			1.7.2.99 Other	
		1.7.99 Other relationship & trust fraud		

Detailed analysis of fraud committed against organizations is beyond the scope of this taxonomy, but these other fraud types would fall into the categories outlined below.
See the Association of Certified Fraud Examiners' (ACFE) "Fraud Tree" (available online) for a detailed categorization of occupational fraud. A corollary project to expand levels 4 and 5 is forthcoming with the ACFE.

Level 1	Level 2	Level 3	Level 4	Level 5
Category 2 Fraud against an **organization**	2.1 Fraud against **government agencies, programs, regulations, and society**	2.1.1 Government Programs	Examples include: Welfare fraud, Disability fraud, Medicare fraud, Medicaid fraud	
		2.1.2 Government Regulations	Examples include: Immigration fraud, Voting fraud, Tax fraud, Stamp fraud	
		2.1.3 Other	Examples include: Insider trading, Environmental fraud	
	2.2 Fraud against **non-governmental businesses or organizations**	2.2.1 Occupational Fraud (committed by internal perpetrator)	Corruption	
			Asset misappropriation	
			Financial statement fraud	
		2.2.2 Fraud committed by external perpetrator	Examples include: Insurance fraud, Bank fraud, Fraudulent suppliers, etc.	