MITRE

Project No.: 840002.01.002.2026.FFF

McLean, VA

MP260217
MITRE PRODUCT

MITRE Fight Fraud Framework™ (MITRE F3™): Design Principles and Methodology

Authors:

Tiffany Bergeron
Michael Cunningham
Allison Robbins
Suneel Sundar

April 2026

Abstract

Preventing fraud is an ongoing challenge for many institutions. Success depends on access to data, insight, and specialized capabilities, but these are often fragmented across cybersecurity, fraud, anti-money-laundering, and other teams. The MITRE Fight Fraud Framework (F3)™ is an authoritative, analyst-developed knowledge base of fraud actor behavior in cyber-based fraud incidents, grounded in real-world tactics and incidents and created by fraud fusion analysts. F3 consolidates key fraud knowledge into a structured, transparent, and operationally relevant resource that focuses initially on financial fraud as experienced by banking institutions.

The framework provides a curated set of tactics and techniques used by fraud actors to fraudulently obtain money, assets, or information from individuals or institutions over cyber channels. It offers a common structure and taxonomy that enables institutions to enumerate the material events of cyber fraud incidents and to partner more effectively on fraud prevention and response. F3 draws on established fraud frameworks and references existing MITRE ATT&CK® cyber techniques where applicable to financial fraud, and it is modeled on the MITRE ATT&CK: Design and Philosophy to ensure quality, traceability, and consistency. This document introduces the motivation behind F3, its design philosophy, the components contained within the knowledge base, and how it can be used and maintained as a living resource for the fraud-fusion community.

Forewords

Fraud is the monetization of crime, and the mechanisms of fraud are becoming increasingly more sophisticated and the crimes more lucrative. Yet attempts to combat fraud are often compromised by the lack of a common framework for describing, detecting, and defeating fraud attempts.

The MITRE Corporation, through its Center for Threat-Informed Defense, developed the MITRE Fight Fraud Framework (F3™) to address this challenge. F3 provides a structured, analyst-driven knowledge base of real-world fraud tactics and techniques to help companies consistently describe and analyze fraud.

F3 leveraged the Cyber Fraud Prevention Framework (CFPF), a fraud taxonomy, lexicon, and framework. The CFPF was created by a working group of sector cybersecurity and fraud experts partnered with the Financial Services Information Sharing and Analysis Center (FS-ISAC) to help firms align teams, improve communication, and strengthen fraud prevention and response efforts. In the collaborative spirit of MITRE ATT&CK®, the working group was pleased to contribute its work to the development of F3 to help all organizations' fraud defense efforts.

As this paper demonstrates, F3 is a reference work and a tool to drive alignment, enhance analytical rigor, and support a more coordinated defense against fraud. This paper outlines its motivation, design philosophy, and core components, and serves as a foundation for its continued evolution.

The near-universal adoption of ATT&CK has proven that a common language is crucial in an evolving threat landscape. To those committed to fighting fraud, F3 will prove instrumental to fostering collaboration, strengthening resilience, and advancing a more unified approach to fraud prevention – rendering companies more effective and the monetization of fraud less successful.

Karen Helmberger
Director of FinTech and Payments

Forewords

Fraudsters thrive in the gaps between our fraud prevention, cybersecurity, and investigative teams. Put four financial institutions in a room, lay out their organizational charts, and you would find four different approaches to fighting fraud-each with different friction points and efficiency gains. Common across all institutions' approaches, however, is that handing off cases, data, and responsibilities between groups creates seams that cybercriminals readily exploit. What's more, they work together to probe our defenses and procedures and scale up attacks as soon as they identify any opportunities. What starts as an isolated problem can snowball into a painful fraud attack in hours.

The Fight Fraud Framework (F3) exists to reduce these gaps. Getting ahead of these attacks requires understanding what tactics and techniques the adversaries employ before they get to the point of monetization. By leveraging this framework, fraud and cyber teams can map what they know about a trend, identify what is not yet known, direct the next steps for their investigation and pursue mitigation efforts across the relevant groups.

Working on this framework with peers across the financial industry and building on the work of the Cyber Fraud Prevention Framework FS-ISAC working group, we put to paper the events that impact our customers and institutions every day. F3 uses an ATT&CK-aligned approach that has proven valuable for communicating how adversaries operate. This framework will evolve alongside the fraud landscape. Still, working on this first version made it very clear that despite different structures, institutional sizes, and roles across industries, there are common attack paths that we can all better defend against.

F3 provides a common language to describe these cyber fraud events and their impact. I hope to see fraud fighters leverage it to not only stop attacks before they impact customers, but also to capture and communicate the underlying tactics and techniques in a consistent way so that teams across industries can "shift left" and stop cyber fraud.

Dan Stiving
Head of Cybercrime & Fraud Intelligence

JPMorganChase

Forewords

"…neither can we, on the other hand, improve a science, without improving the language or nomenclature which belongs to it." - Antoine Lavoisier, Élémentaire de Chimie (Elements of Chemistry), 1789

According to the 2026 NASDAQ Global Financial Crime Report, financial fraud losses were estimated at $579B in 2025. The latest FBI IC3 Report reported $17.6B of losses impacting Americans. This problem is not only growing, it is growing faster. The need to fight this threat has never been more urgent.

The emergence of decentralized currency markets, the growth of digital payments, and the ease of impersonation via generative AI have formed a confluence of conditions where financial fraud can thrive. We must turn the tables and make this environment defensible, resilient, and ultimately, hostile to crime. However, defending our global financial system requires broad collaboration between organizations and across multiple domains. Without clear communication and common terms, we will struggle to keep up.

Fraud depends on confusion and misidentification. Thus, as we develop defenses against fraud, it is imperative that we identify, name, describe, and categorize its components. Only by building such an ontology can we share intelligence, test theories, and iterate on solutions. This is the idea behind the MITRE Fight Fraud Framework: to properly represent the techniques of financial fraud, while connecting directly with frameworks like MITRE ATT&CK to reflect associated cyber tactics and techniques.

Financial fraud is a dynamic and pervasive threat, one which will not be solved by a single policy or technology. The solutions will depend on our ability to communicate, to experiment, and to learn as a community. The Fight Financial Fraud Framework helps to establish that foundation, and we are proud to be a part of it.

Matt Berninger
Senior Vice President, Cyber Risk Intelligence Center

MARSH

Preface

This paper documents the initial published version of MITRE F3 as of April 2026. F3 will evolve and expand over time. This paper will be maintained as a living document and will be updated as significant changes are made to F3 and/or the process used to maintain the content within F3. For the most up-to-date information, refer to the F3 website: https://ctid.mitre.org/fraud.

Acknowledgements

The MITRE Fight Fraud Framework (F3)™ was developed through MITRE's Center for Threat-Informed Defense (CTID) and CTID member-powered collaboration. With the understanding that the challenges we face are bigger than ourselves, our members join CTID prepared to tackle hard problems in a uniquely collaborative environment. CTID gratefully acknowledges the significant contributions and deep expertise provided by Aviation Information Sharing and Analysis Center (A-ISAC), Citigroup, CrowdStrike, Financial Services ISAC (FS-ISAC), JPMorganChase, Lloyds Banking Group, Marsh, National Retail Federation (NRF), Retail & Hospitality ISAC (RH-ISAC), Standard Chartered, and Verizon Business towards the development of MITRE F3™. CTID further recognizes Group IB as a key data contributor whose insights and contributions supported the development of F3.

Table of Contents

List of Figures

List of Tables

1 Introduction

The MITRE Fight Fraud Framework (F3) is a curated knowledge base of tactics, techniques, and procedures (TTPs) used by fraud actors in cyber-based financial fraud incidents. These incidents involve the intentional use of deceptive or illegal practices to fraudulently obtain money, assets, or information from individuals or institutions and include actions carried out over cyber channels. MITRE F3 includes behaviors that characterize known fraud TTPs used in the commission of these incidents and references existing MITRE ATT&CK cyber techniques as applicable to financial fraud. F3 provides a living knowledge base of fraud actor TTPs based on real-world observations of cyber fraud incidents. The initial release focuses on financial fraud as seen by banking institutions[1].

At a high level, F3 is a behavioral model that consists of the following core components:

- Tactics, denoting short-term, tactical fraud actor goals during an attack;
- Techniques, describing the means by which fraud actors achieve tactical goals; and
- Sub-techniques, describing more specific means by which fraud actors achieve tactical goals at a lower level than techniques.

This relatively simple representation strikes a useful balance between sufficient technical detail at the technique level and the context around why actions occur at the tactic level.

F3 will evolve over time as fraud actor TTPs evolve and new behaviors are identified. New information relevant to fraud TTPs can come from many different sources, including fraud incident reports and contributions from the fraud community.

2 Background

Preventing fraud is an ongoing challenge for many institutions. Banking institutions in particular are regulated by the government and are legally required to follow Anti-Money Laundering (AML) rules and regulations under laws like the Bank Secrecy Act. These institutions must conduct due diligence (i.e., Know Your Customer or KYC), monitor transactions to detect and prevent illegal activity, and report suspicious activities to the proper authorities. Success depends on access to data, insight, and specialized capabilities, but these are often fragmented across cybersecurity, fraud, anti-money laundering, and other teams.

[1] A banking institution is a type of financial organization that is legally authorized to provide the public with services and products related to money, such as deposit accounts and loans.

F3 was created by and for fraud-fusion analysts to help teams coordinate and focus their anti-fraud efforts using a shared, consistent language. By anchoring the framework in actual fraud incidents, it ensures the knowledge base remains closely aligned with real-world threats that analysts are likely to encounter over the course of a cyber fraud incident.

F3 is grounded in real-world fraud actor behavior derived from existing fraud frameworks and developed by fraud fusion analysts. The framework is modeled after ATT&CK, inspired by the *MITRE ATT&CK: Design and Philosophy*[2], to enumerate fraud actor behavior. F3 includes new content to describe fraud technical behaviors for which there is no existing ATT&CK content, and references and refines existing ATT&CK techniques when they are applicable to financial fraud. The initial release focuses on financial fraud as seen by banking institutions.

3 The F3 Model

Fraud incidents contain cyber artifacts that can be used to find future fraud, and F3 provides that fusion of cyber and fraud data sources into tactics and techniques specific to fraud incidents. The framework provides a collective ability to enumerate the material events of a fraud incident and to implement controls that disrupt fraud through emulating, detecting, and preventing the TTPs used in these incidents. Key aspects of the F3 model are:

- Common structure and taxonomy
- Partnership on fraud prevention and response
- Shared indicators among institutions

The basis of F3 is the set of techniques and sub-techniques that represent actions that fraud actors perform to accomplish objectives. Those objectives are represented by the tactic categories that the techniques and sub-techniques fall under. This relatively simple representation strikes a useful balance between sufficient technical detail at the technique level and the context around why actions occur at the tactic level.

3.1 Design Principles

F3 was developed using a set of clear design principles, informed by the practical experience of fraud fusion analysts and applied to define its tactics, techniques, and sub-

[2] The MITRE Corporation (2015-2025). *MITRE ATT&CK: Design and Philosophy*. https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf

techniques. These design principles form the conceptual foundation of the methodology used to create F3 and will continue to guide its maintenance and future enhancement.

Fraud methods will evolve over time and additional knowledge will be gained. The F3 development process will remain focused on accurately representing how fraud actors operate, through following these design principles and providing information in a way that makes it easy to categorize fraud actor actions and relate those actions to defenses. This enables defenders to consistently describe, detect, and prevent fraud incidents using a common, structured approach.

There are four Design Principles that are core to the development of F3:

- Design Principle #1: The financial institution must see the effects of a technique during the fraud incident.
- Design Principle #2: The fraud incident must contain a cyber-based technique.
- Design Principle #3: Techniques must describe the behavior of the fraud actor.
- Design Principle #4: For behaviors with the same "how" performed in different ways, we must create a technique/sub-technique relationship.

Fraud methods will evolve over time and additional knowledge will be gained. The F3 development process will remain focused on accurately representing how fraud actors operate, through following these design principles and providing information in a way that makes it easy to categorize fraud actor actions and relate those actions to defenses. This enables defenders to consistently describe, detect, and prevent fraud incidents using a common, structured approach.

3.1.1 Design Principle #1: The institution must see the effects of a technique during the fraud incident.

The institution must be able to observe and understand how a technique impacts a fraud incident. Seeing how the behavior or action fits in the overall outcome of the fraud incident is needed so that its effectiveness, limitations, and side effects can be accurately evaluated and used to improve future strategies for mitigating and detecting the behavior.

Visibility into what the fraud actor does during each step of a fraud incident provides a clear understanding of their methods and behaviors. This insight can then be used to inform and shape future fraud strategies, rules, and processes, helping organizations better prevent, detect, and respond to similar threats in the future.

3.1.2 Design Principle #2: The fraud incident must contain a cyber-based technique.

The fraud incident must involve the use of a cyber-based technique as an element of how the fraud is carried out. This means the fraud incident includes use of digital or technological methods, such as phishing, malware, unauthorized access to information systems, or other forms of cyber manipulation, rather than being solely physical, social, or paper-based in nature. The requirement to contain a cyber artifact is for analysts to use to help detect future fraud attempts.

The purpose is to provide actionable support for cyber threat intelligence, detection engineering, security control implementation, and performing investigations. This ensures that insights are not only understood but can be effectively applied to strengthen an organization's overall security posture.

3.1.3 Design Principle #3: Techniques must describe the behavior of the fraud actor.

Techniques represent 'how' a fraud actor achieves a tactical goal by performing an action. Each technique captures a distinct, observable action or behavior that is used by the fraud actor to achieve their objective. A technique is not an entity or a tool, but rather the specific way those entities or tools are used. Techniques focus on actions known to be used by threat actors, represented by standardized terms.

Defining techniques in this way enables clear recognition and consistent categorization of fraud behaviors within an incident. This also provides operational value by ensuring that defenses such as detection logic and security control design can be mapped to the actions performed by fraud actors, rather than to the specific entities or tools used to achieve their goals.

3.1.4 Design Principle #4: Behaviors with the same "how" performed in different ways must use a technique/sub-technique relationship.

Not all techniques will have sub-techniques. Sub-techniques describe more specific means by which fraud actors achieve tactical goals at a lower level than techniques. Sub-techniques further break down behaviors described by techniques into more specific descriptions of how behavior is used to achieve an objective.

Techniques provide a high-level, manageable view of fraud behavior, while sub-techniques provide the additional detail needed for demonstrating the many ways that techniques are

performed. This structure helps to reduce overlap and allows for a similar abstraction level of techniques across the framework, capturing variations and lower-level details as sub-techniques.

3.2 The F3 Matrix

The relationship between tactics, techniques, and sub-techniques can be visualized in the F3 matrix[3]. Figure 1 depicts the F3 Matrix:

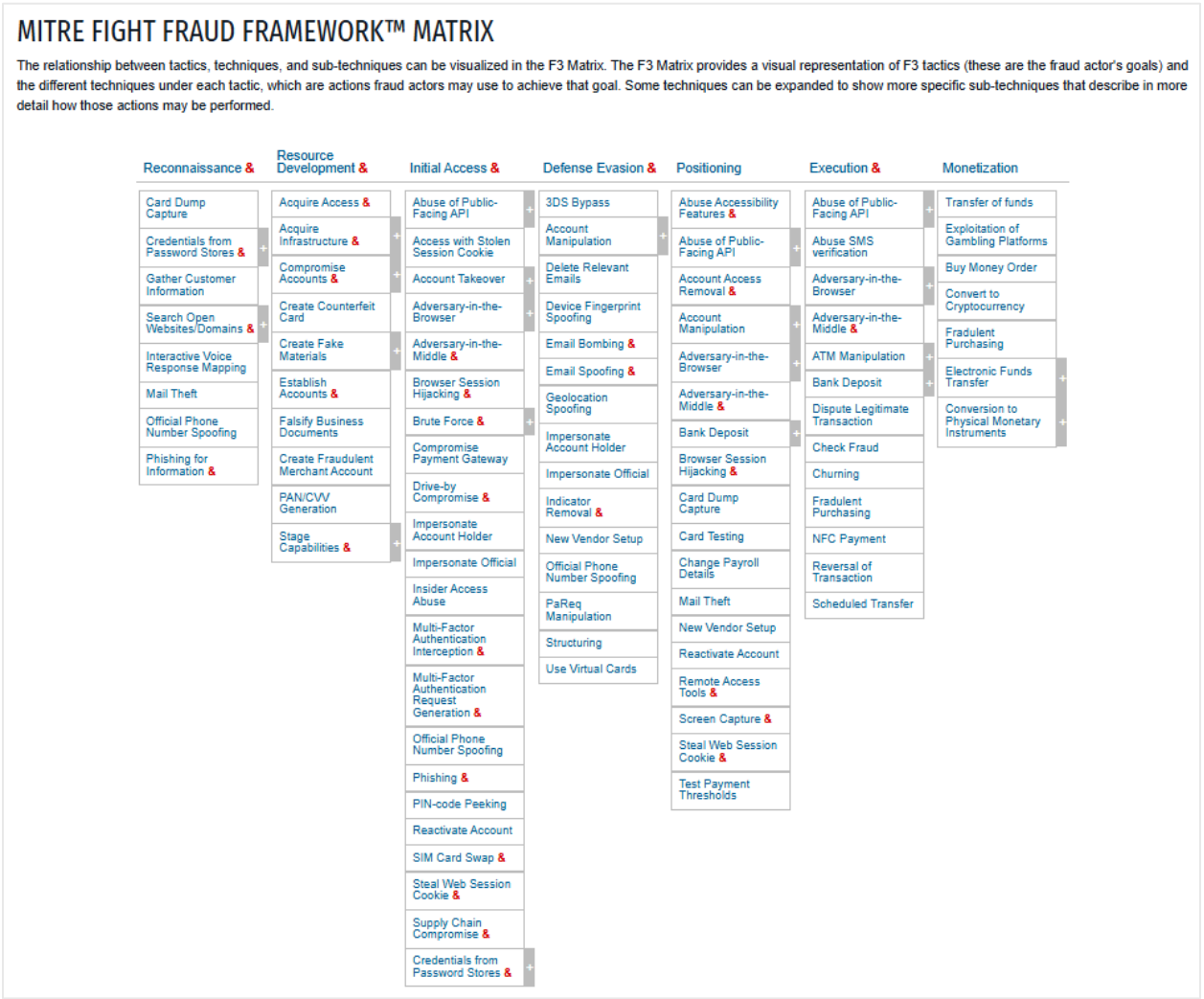

Figure 1: F3 Matrix Overview

[3] MITRE Center for Threat-Informed Defense (April 2026). *MITRE Fight Fraud Framework™ Matrix*. https://ctid.mitre.org/fraud/matrix

For example, under the Resource Development tactic (this is the fraud actor's goal, to prepare for fraud in the target environment), there are a series of techniques including Acquire Infrastructure and Create Fake Materials. Each of these is a single technique that fraud actors may use to achieve the goal of setting up infrastructure and capabilities to support fraud activities.

Furthermore, some techniques can be broken down into sub-techniques that describe in more detail how those behaviors can be performed. For example, Create Fake Materials has two sub-techniques, Fake Documents and Fake Website, to describe how forged or fraudulent resources may be created to support attempted fraud. Figure 2 depicts the Acquire Infrastructure and Create Fake Materials techniques under the Resource Development tactic, expanded to show their respective sub-techniques.

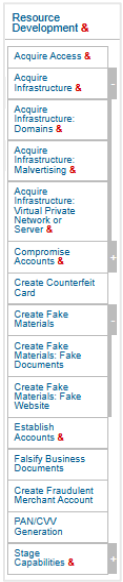

Figure 2: Examples of Expanded Techniques

3.3 Tactics

Tactics represent the "why" of an F3 technique or sub-technique: the fraud actor's tactical goal and the reason for performing an action. Tactics are not the same as phases of a fraud incident and not every tactic will be present in every fraud incident.

F3 is composed of seven tactics, as described in Table 1 below:

Table 1: MITRE F3 Tactics and Descriptions

Tactic	Tactic Description
Reconnaissance	The fraud actor's actions to gather information they can use to plan future operations, including both cyber intrusions and attempted fraud. Reconnaissance consists of techniques that involve fraud actors actively or passively gathering information that can be used to support targeting. Such information may include details of the victim organization, infrastructure, or staff/personnel. This information can be leveraged by the fraud actor to aid in other phases of the fraud lifecycle, such as using gathered information to plan and execute Initial Access, to scope and prioritize post-compromise objectives, or to drive and lead further Reconnaissance efforts.
Resource Development	The fraud actor's actions to establish resources they can use to support both cyber and fraud activities. Resource Development consists of techniques that involve fraud actors creating, purchasing, or compromising/stealing resources that can be used to support targeting. Such resources include infrastructure, accounts, or capabilities. These resources can be leveraged by the fraud actor to aid in other phases of the fraud lifecycle, such as using purchased domains to support Execution, email accounts for phishing as a part of Initial Access, or spoofing to help with Defense Evasion.
Initial Access	The fraud actor's actions to gain a foothold in a selected environment. Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a selected environment. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses in browsers. Footholds gained through initial access may allow for continued access, like compromise accounts and use of external remote services, or may be limited-use due to changing passwords.
Defense Evasion	The fraud actor's actions to avoid being detected. Defense Evasion consists of techniques that fraud actors use to avoid detection throughout their compromise. Techniques used for defense evasion include phone number spoofing or social engineering. Fraud actors also leverage and abuse trusted processes to hide and masquerade their activities. Other tactics' techniques are cross listed here when those techniques include the added benefit of subverting defenses.

Positioning	The fraud actor's actions in a selected environment, after initial access, to collect or manipulate data or otherwise prepare for execution. Positioning consists of techniques that involve fraud actors gathering sensitive information, altering account configurations, manipulating transaction parameters, or establishing conditions necessary for successful fraud operations. These preparatory activities enable fraud actors to maximize the value extracted during fraud execution or establish persistent access for future operations.
Execution	The fraud actor's actions to run malicious code or initiate fraudulent transactions that will convert stolen data to money. Execution consists of techniques that result in fraud actor-controlled code or actions running on a local, remote, or transaction-processing system. Techniques that run malicious code or automate actions are often paired with other tactics to achieve broader goals, such as exploring a network, manipulating applications, initiating unauthorized payments, or altering transaction data to support fraud. For example, a fraud actor might use a remote access tool to run a PowerShell script that performs Remote System Discovery and then launch scripts or bots that submit fraudulent transfers, modify payment instructions, or replay payment messages through compromised banking or merchant platforms.
Monetization	The fraud actor's actions to convert assets, often stolen, into usable funds or value in their possession. Fraud actors may convert fraudulently obtained funds or assets into a form they can utilize or transfer to their possession. Monetization consists of techniques that involve fraud actors liquidating stolen digital assets, transferring funds from compromised accounts, converting fraud proceeds into difficult-to-trace monetary instruments, or manipulating markets. These techniques represent the final stages of fraud operations where fraud actors secure their gains and attempt to obscure the transaction trail.

3.4 Techniques and Sub-Techniques

Techniques represent “how” a fraud actor achieves a tactical goal by performing an action. There may be many ways, or techniques, to achieve tactical goals or objectives, resulting in multiple techniques in each tactic category. Likewise, there may be multiple ways to perform a technique, resulting in distinct sub-techniques under a technique. In addition, a

single technique can be used to achieve multiple goals, meaning a technique can be listed under multiple tactics.

Sub-techniques further break down behaviors described by techniques into more specific descriptions of how behavior is used to achieve an objective. The purpose behind sub-techniques is to provide more detail on how techniques can be used. Not all techniques have sub-techniques. There are several techniques that do not have a natural breakout into sub-techniques or do not make sense to generalize into higher level techniques.

3.5 Versioning

F3 uses a system for versioning objects (e.g., techniques, sub-techniques), the matrix view, and releases. The system is designed to inform users when parts of F3 have changed, give an indication as to the degree of the change, allow users to differentiate between versions of the matrix, and have stable references for content releases.

Versions will only increment between content releases. That means that if two changes are made to a technique between scheduled updates, then the version will only increase once.

3.5.1 Objects

Objects in F3 refer to any item in the knowledge base that can have a relationship with another object. Each has their own criteria for how versions are incremented between releases.

All objects are assigned a two-part numerical version MAJOR.MINOR that starts at 1.0 for any new object.

3.5.1.1 Techniques and Sub-Techniques

For techniques and sub-techniques, major version changes should happen infrequently. Major version changes consist of:

- Name changes: modifications to the word or set of words used to identify and distinguish the technique or sub-technique.
- Scope changes: modifications of how the technique could be interpreted or what it covers or does not cover in the description, or changes to associated tactics.

Minor version changes to techniques and sub-techniques consist of:

- Descriptive information changes: modifications such as minor updates that do not change the scope, procedure examples, detections, mitigations, and references.

3.5.1.2 Tactics

Since tactics represent the tactical goals of a fraud actor, these remain relatively static over time because fraud actors' goals are unlikely to change. There may be cases where tactics need to be refined or created for better definition of what fraud actors are trying to accomplish by performing certain actions.

3.5.2 Matrix

Each matrix that appears on the F3 website is assigned a numerical MAJOR.MINOR as its version number.

3.5.3 Releases

A release occurs when the changes to the STIX representation of F3 are bundled and released along with any updates to the F3 website. Prior versions of the content and website will be saved and stored for historical reference.

4 The F3 Methodology

The previous sections of this document have described and defined the purpose and structure of the F3 knowledge base. This section describes the components of the methodology used in the creation of F3. It also describes the process recommended to determine if and when new tactics or techniques should be added to the knowledge base.

The information within F3 will evolve over time, as will the considerations used for what information gets included and how it's structured. The process is as much of an art as it is a science. The focus remains on providing an accurate representation of how fraud actors conduct operations in a way that is easy to categorize the actions they take and to relate those actions in a way that defenders can use to describe, prevent, and detect and/or stop them.

4.1 Conceptual

There are three conceptual ideas that are core to the philosophy behind F3:

- Maintain the fraud actor's perspective.
- Follow real-world use of fraud activity.
- Apply a usable level of abstraction.

4.1.1 Fraud Actor Perspective

F3 takes on the perspective of the fraud actor in its terminology and descriptions for tactics and techniques described in the model. Use of the fraud actor's perspective makes it easier to understand actions and potential countermeasures in context than it would from a purely defense perspective. Defenders are then able to follow the fraud actor's motivation for individual actions and understand how the actions and dependencies relate to specific classes of defenses that may be deployed in an environment.

4.1.2 Empirical Use

Empirical use refers to action based on direct observation, experience, or experiment rather than theory. F3 is based upon real-world cyber and fraud data sources, including the experience and broad knowledge of fraud analysts, fused into a common language of tactics and techniques specific to cyber fraud incidents.

The activity described by F3 is drawn from fraud actor TTPs that have been used in cyber fraud incidents, which provides a grounding for the knowledge base so that it accurately portrays activity happening or likely to happen in the wild. The tie to incidents keeps the model grounded to real-world threats that are likely to be encountered rather than theoretical techniques that are unlikely to be seen due to difficulty of use or low utility.

4.1.2.1 Sources of Information

F3 also includes derivation from prior work. Fraud activities documented in other fraud models were analyzed through empirical use examples and fused:

- FS-ISAC Cyber Fraud Prevention Framework
    - Framework that enables gathering and sharing of cyber fraud information across the financial sector regarding fraud conducted on cyber channels
- National Retail Federation Retail Fraud Taxonomy
    - Framework for assessing and categorizing retail fraud threats and identifying appropriate actions to mitigate them
- Group-IB Cyber Fraud Intelligence
    - Framework to systematically break down fraud actor actions and behaviors across an incident into stages and techniques
- Stripe Fraud Tools Tactics and Techniques (FT3)
    - Framework to enhance understanding of the tactics, techniques, and procedures (TTPs) used by actors in fraudulent activities

4.1.3 Abstraction

The level of abstraction for fraud actor tactics and techniques within F3 is modeled in a way to be appropriate to bridge offensive action with defensive countermeasures. The tactics and techniques in F3 are behavior-based and provided in the context of individual actions fraud actors make and which actions can be used to achieve a goal. Defining the actions used in fraud incidents in this way provides a common taxonomy of individual actions and goals that can be understood by both offensive and defensive teams for more effective fraud prevention.

4.2 Tactics

Tactics represent the tactical goals of a fraud actor. The tactics in F3 will remain relatively static over time since what the fraud actors are trying to accomplish is unlikely to change. There may be cases where tactics need to be refined for better definition of the actions occurring. New tactics will follow the need to define existing, but uncategorized, or new fraud goals to provide accurate context for what a fraud actor is accomplishing by performing a technique action.

4.2.1 Naming and Identifier Conventions

Tactics are assigned identifiers or IDs, names, and descriptions to describe their specific information. Additional entities, such as references, may be added in future versions of F3.

4.2.1.1 Identifiers (IDs)

F3 tactics are of the format FA#### and are unique within the knowledgebase; or, if a tactic already exists in the ATT&CK knowledgebase, the ATT&CK identifier is used (i.e., TA####). The identifiers are assigned to ensure machine readability and compatibility with related MITRE and other frameworks and tools, such as ATT&CK and STIX.

4.2.1.2 Names

Tactic naming conventions focus on the “why” or the tactical objective of the fraud actors that make it unique. The names are meant to be useful contextual categories for human readability and reference.

4.2.1.3 Descriptions

Tactic descriptions provide a definition describing the category and serve as a guide for what techniques should be within the tactic. This includes the fraud actor’s tactical objective or reason for performing an action.

4.3 Techniques and Sub-techniques

Techniques and sub-techniques are the foundation of F3 and represent the individual actions fraud actors take. The Design Principles are applied in the decision process to create a technique or sub-technique and contribute to their respective details within the knowledge base.

Technique names focus on the aspect of the technique that makes it unique: what the fraud actor achieves at an intermediate level of abstraction from using the tactic. Sub-techniques often signify how a technique is used at a lower level of abstraction. Industry-accepted terminology tends to be used if a technique or sub-technique is already established and documented (e.g., in ATT&CK).

When a potential new behavior is identified, it may be included in F3 by:

- Adding an entirely new technique,
- Adding a new sub-technique under an existing technique, or
- Enhancing or abstracting an existing technique or sub-technique

The decision will require consideration of whether the newly identified or previously uncategorized behavior is similar to other techniques and how, if it naturally fits under a similar technique as a sub-technique, and if the new behavior would conceptually be treated differently by F3 users (e.g., incident description, defensive measures). If a new behavior is not conceptually different in how it is implemented or defended against, then it likely should be included in an existing technique or sub-technique.

4.3.1 Naming and Identifier Conventions

Techniques and sub-techniques are assigned identifiers or IDs, names, and descriptions to describe their specific information. Additional entities, such as references, may be added in future versions of F3.

4.3.1.1 Identifiers (IDs)

F3 technique and sub-technique identifiers are of the format F#### for techniques and F####.### for sub-techniques and are unique within the knowledgebase; or, if a technique or sub-technique already exists in the ATT&CK knowledgebase, the ATT&CK identifier is used (i.e., T####, T####.###). The identifiers are assigned to ensure machine readability and compatibility with related MITRE and other frameworks and tools, such as ATT&CK and STIX.

4.3.1.2 Names

Technique naming conventions focus on the actions fraud actors take that make it unique to achieve their tactical goals. Sub-technique names typically signify how a technique is used at a lower level of abstraction. The names are meant to serve as useful contextual designations for human readability and reference.

4.3.1.3 Descriptions

Technique and sub-technique descriptions provide explanatory information about the technique or sub-technique. This includes what the action is and what fraud actors typically use it for. Descriptions may also indicate how a fraud actor can take advantage of it or variations of how it could be used.

5 Usage

Collaboration and shared understanding across teams is highly important to effectively combat financial fraud. Responsibility for detecting, investigating, and responding to financial fraud may be spread across multiple groups within an organization, and each may have its own tools, processes, and terminology. F3 is designed to bridge these gaps by giving all stakeholders a common language for describing fraud incidents, behaviors, and countermeasures. Through this shared model, teams can coordinate more effectively and align their efforts.

The following scenario demonstrates how F3 enables teams to work together:

- Fraud analysts produce F3-based fraud incident reports and share actionable fraud intelligence.
- Offensive security operations teams identify and validate detections for F3 techniques.
- Defensive detection engineers implement countermeasures for techniques observed in fraud incidents.
- Security officers report suspected fraudulent activity using the F3 model.

Fraud team use of F3 goes beyond identification of the fraud actor's actions taken during the cyber fraud incident. In response, the fraud team may also recommend a combination of organizational efforts, such as:

- New fraud-related rules, such as temporarily lowering transaction limits or introducing additional verification for higher transfers.

- A customer notification campaign, which may include warnings about social engineering attempts or instructing customers on password security.
- Targeted training is provided to the workforce including contact center agents and branch staff to recognize fraud indicators and escalate suspected cases of account takeover.
- Adjusted dispute handling workflows to rapidly work with impacted customers while preserving evidence needed for investigation.

This shared foundation strengthens coordination across teams and helps institutions to work cohesively to maintain a secure financial environment. Users of F3 will encompass many roles and responsibilities associated with organizational cyber defense, fraud prevention and detection, and incident response. These include:

- Fraud Incidents: Create detailed incident reports using F3 to describe fraud actor goals, behaviors, and impacts.
- Fraud Intelligence: Use the F3 common language to structure, compare, and analyze reported fraud intelligence.
- Defensive Measures: Apply recommendations for aligning operational defensive measures to protect from threats contained in F3 and mitigate financial fraud.
- Information Sharing: Share intelligence on threats and fraud techniques with other institutions as described with F3 to strengthen industry-wide defense.

6 Summary

This document provides the motivation behind the creation of F3, its design philosophy, the components contained within the knowledge base, and how it can be used. It is meant to be used as an authoritative source of information about F3, as well as to help guide how the framework is expanded and maintained. By defining what the framework contains and how it should be maintained, the document helps ensure consistency, clarity, and alignment as the framework evolves over time.

F3 is grounded in real-world fraud actor behavior and developed by fraud fusion analysts. Existing fraud frameworks were used as foundational inputs, and the methodology and principles used by ATT&CK were used as a model to derive this knowledge base of real-world fraud actor behavior. This combination of real threat data and a proven analytical approach gives users greater transparency into how the framework was constructed, increases confidence in the information it provides, and demonstrates how it can be applied by the fraud-fusion community.