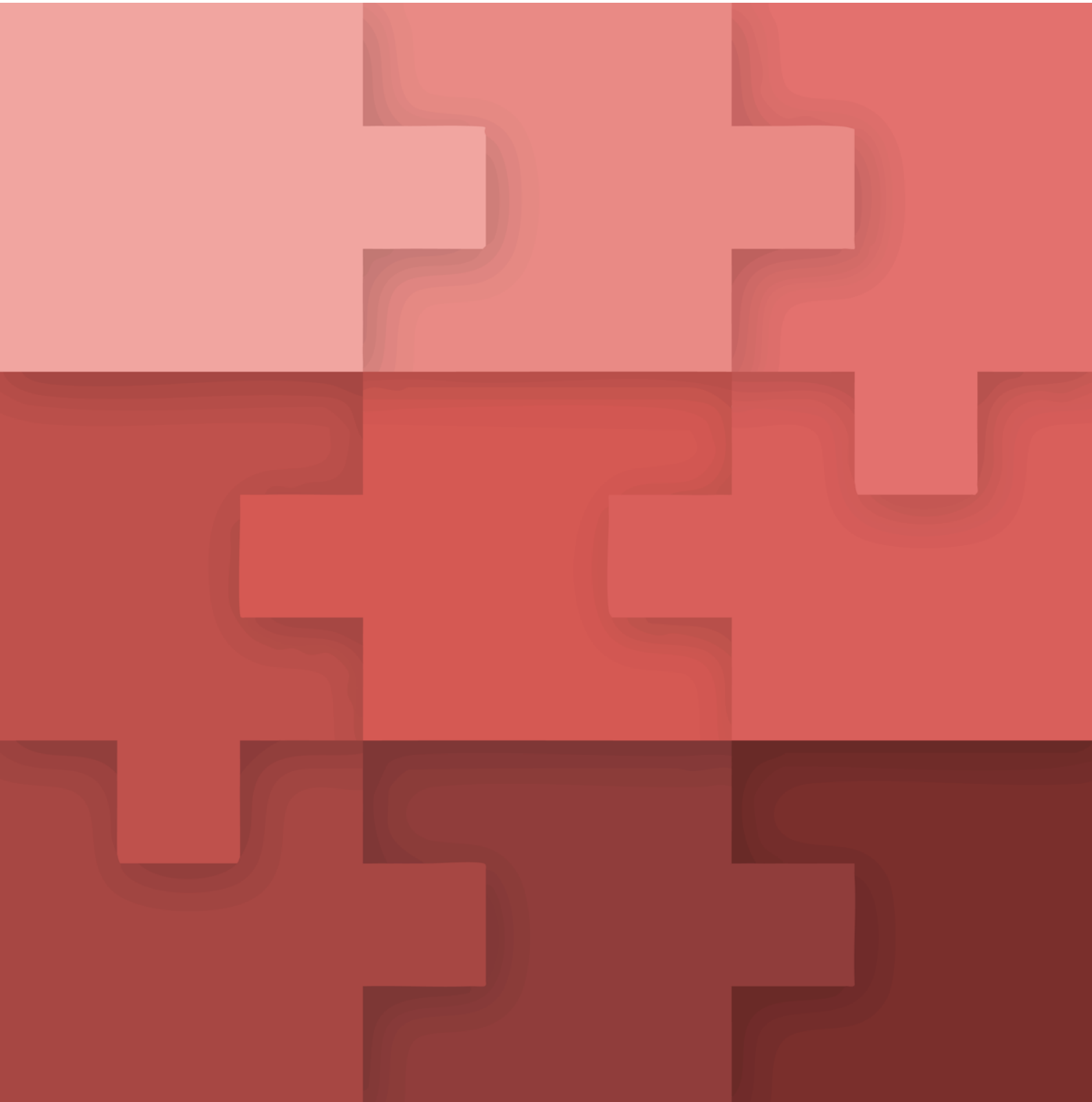
Fraud Kill Chain

White Paper V2

April, 2025



1 CONTENT

1 Content 2

2 Preface 4

2.1 Reading guide 4

3 Introduction 5

4 Fraud Attack Chains 7

4.1 Background 7

4.2 Economic Crime Lifecycle and Components 8

4.3 Assembly of the Typology 12

4.4 Completing the Typology 12

4.5 Full Typology Usage Example 13

5 Framework Components 14

5.1 Full Framework 14

5.2 Framework Example 15

6 Challenges / Considerations 17

6.1 Alternatives 17

6.2 Compatibility 17

6.3 Adoption 17

6.4 System Integration 17

6.5 TTP / IOC Standardization 18

7 Glossary 18

8 Evolution 19

9 The April 2025 Fraud Kill Chain 20

9.1 Reconnaissance 21

9.2 Resource Development 21

9.3 Psychological Manipulation 21

9.4 Faux Communications 22
9.5 Credential Compromise 22
9.6 Account Access 23
9.7 Authorization Compromise 23
9.8 Fraud Event 24
9.9 Monetization 24
9.10 Money Laundering 25

2 PREFACE

This document represents the initial white paper that kick-started the development of the Fraud Kill Chain. The white paper has initiated collaboration among various financial institutions, consultancy firms, and subject matter experts, setting the foundation for what is evolving as comprehensive framework. The taxonomy and terminology introduced in this pioneering document have undergone evolution, continually enhanced by additional layers and Techniques, Tactics, and Procedures (TTPs). Over time, these collaborations and iterative developments have refined the framework, making it more robust and versatile to address the complex and dynamic nature of fraud and financial crimes.

The Fraud Kill Chain and this associated white paper are used in real-world operational Fraud and Fusion departments. But they may serve as an inspiration for further development, too.

If you're reading this, and have ideas on how to improve or append, we'd love to hear your ideas. No version of the Fraud Kill Chain is ever final, and collaboration among fraud and fusion professionals is paramount.

Visit www.fraudkillchain.com for more information on how to connect to the community.

2.1 READING GUIDE

Chapter 1-2: Content & Preface

Chapter 3-7: Initial white paper

Chapter 8-9: April 2025 Fraud Kill Chain

3 INTRODUCTION

Cyber, Fraud, and Financial Crime threats are proliferating across the financial landscape as economic activity increasingly globalizes, threat actors are able to obtain and deploy increasingly sophisticated tools, and backend transaction infrastructure becomes increasingly real-time. In this environment, Financial Institutions spend significant resources identifying, interrupting, and responding to a constantly evolving array of threats. attacks, and economic crimes.

Financial Institutions face a relentless need to be informed and incorporate every resource available to maximize their capabilities and remain current in their ability to identify and interdict cyber and economic crimes. The broader financial industry has responded to this critical need through several different avenues, such as information sharing networks, inter-company data exchanges, industry certifications and standards, and frameworks to expedite the communication and understanding of attack and criminal patterns.

To highlight the last item, frameworks have significant value in helping organizations and the personnel responsible for mitigating and responding to attacks and crimes to understand and contextualize the specific elements of a threat and more rapidly prepare or stop the activity.

Framework development, deployment, and usage has grown over the last few decades. For example, in light of the US Department of Defense's recognition that cyber warfare is the 5th column of warfare, the cyber industry has responded by releasing of a few different cyber-focused frameworks, including Lockheed Martin's Cyber Kill Chain, MITRE ATT&CK, and the Diamond Model.

These frameworks have had a demonstrable and positive impact on the Cyber industry by providing specialists and stakeholders a structured mechanism to document and organize the features of cyber-related behavior and more efficiently communicate the details to other organizations. This greatly expedites the ability to understand and act on a cyber threat.

While the cyber industry demonstrated the success of these frameworks, the fraud and traditional financial crime industries face a challenge with the existing frameworks. These frameworks are usually very technical in nature, and don't allow for comprehensive descriptions of behavioural manipulation, which are prevalent in financial crime, resulting in few available frameworks that accomplish the same vision as the Cyber-oriented methods within the context of financial crimes .

Additionally, the "lack of a shared vocabulary" afforded by a standardized framework and method slows down information sharing across institutions and stakeholders in the financial services industry, and has adverse effects on the ability and speed of analyzing and mitigating new types of economic crime.

These factors demonstrate a need in the Fraud and Financial crime space for a framework that can be used to assist organizations and participants to document fraud and economic crimes behaviors and attacks in a more structured format, and more easily and effectively

communicate those behaviors to other fraud and financial crimes across the financial services industry.

This framework builds upon and extends the concepts of other frameworks and offers a focused framework for Fraud and Financial Crime events. The goal of this framework is to foster knowledge and familiarity with fraud and economic crime threats and enhance the ability for institutions to effectively share and coordinate methods to stop, interdict, prevent, and/or deter threats.

4 FRAUD ATTACK CHAINS

4.1 BACKGROUND

4.1.1 FRAUD & ECONOMIC CRIME CHALLENGE

Financial Institutions are constantly subject to a wide range of fraud and economic crime attacks, and many of these attacks share many common traits regardless of the size or geography of the institution. Operating independently, institutions must often consider these attacks and events in isolation, relying on the collective experience and skills of staff, and limited information exchanged between institutions.

Additionally, as institutions internally discuss and coordinate on fraud events across the organization, different levels of experience and familiarity with fraud and economic crimes can create barriers to responding rapidly and effectively. In the worst cases, communication and coordination challenges created from information asymmetry can create silos and reinforce local actions instead of cross-organization coordination actions.

To address these environmental concerns, Institutions and stakeholders would be well served by a system that not only standardizes the description and details of a fraud and economic crime event, but also facilitates education and understanding of the event and its contextual factors. Such a system would reduce silos and enhance cooperation by fostering a common understanding across the entire organization, regardless of background and current operating focus.

4.1.2 ATTACK AND EVENT COMPLEXITY CHALLENGE

Fraud and economic crime attacks and events take many different forms, ranging from complex mobile malware exploits to traditional money mule activities. With such a range of potential different attacks and events, organizing, structuring, and tracking the event itself and the organization functional, technical, operational, and control response can be a daunting and resource-intensive effort.

Further, as attacks evolve or entirely new attacks and events happen, the organization may lose sight of prior and in-flight efforts as various operating groups pivot to address acute and tactical needs. As a result, many organizations suffer with limited documentation for their cyber, fraud, and economic crime programs, and are left to overly rely on existing systems and controls over a more comprehensive, strategic approach.

The limited organization and documentation create an environment where attack or event information shared from other organizations or industry partners, requires a substantive effort to review existing systems and controls to determine if the organization has a response posture in place, let alone the details about how they prefer to respond and handle such events.

To address this, Institutions and their stakeholders would be well served by a system that enables a consistent display of the structure and context of an attack or event, in addition to enabling the organization to document, track, and trace their controls and response posture to the attack or event.

4.1.3 INTER-ORGANIZATION DATA EXCHANGE

In addition to descriptive and communicative challenges with attacks and events, there is also a challenge with communicating and coordinating response across different financial institutions and stakeholders in the financial services market. Without a common typology and framework, institutions create bespoke methods to communicate the risks, impacts, and mitigation strategies for attacks and events.

The variable nature of these communications between organizations further complicates effective management of fraud and economic crimes, as non-originating institutions must often decode and understand the actionable parts of an advisory. Additionally, the variability often results in critical factors being lost in translation between organization; factors that can significantly affect the financial and operational exposure an institution may face.

Institutions would be well-served by a system that organizes and facilitated cross-institution communication through a consistent terminology, topology, and actionable detail. With this system in place, institutions can more rapidly understand the details of the attack or event, compare it to their existing control and operating environment, and more rapidly enhance their response and control posture, which limits loss and a degradation of customer experience.

4.2 ECONOMIC CRIME LIFECYCLE AND COMPONENTS

4.2.1 ATTACK / EVENT LIFECYCLE

Economic Crime attacks and events can take many different forms, involve many different participants, and touch a myriad of systems and processes. Even with the potential for a nearly endless combination of elements, the lifecycle can be conceptually distilled into three stages:

- **Initiation**: The preparation and initial activities a threat actor performs to begin execution to achieve their attack or event goals
- **Execution**: The core activities performed by a threat actor to achieve the economic crime.
- **Extraction**: Actions taken by the attackers to obtain the results or financial benefits of the economic crime.

This simple 3 stage approach can be flexibly applied to a wide range of economic crimes, from fraud-oriented attacks like application fraud and account takeover to other economic crimes like money laundering and circumventing sanctions.

The 3-stage approach provides a foundation for us to further develop an economic crime typology, through the exploration of each stage and components that would exist within each.

4.2.2 INITIATION STAGE

4.2.2.1 SUMMARY

Economic Crime attacks and events all have a starting point. The initiation stage is where the threat actor begins the overall process, typically by identifying a target, engaging with the target, and begin the first steps of the attack.

Attackers must be diligent throughout the initiation phase, as all downstream activities depend on a successful initiation. This is also the stage where financial institutions have an opportunity to educate and equip customers to help disrupt the attack chain right at the start.

4.2.2.2 STAGE FOCUS

The initiation stage is focused on the target and the method of the attack.

4.2.2.3 EXAMPLES

An example of the initiation phase is the identification and gathering of personal information to compromise a customer's account in a takeover. Another example is the acquisition and testing of credit card data to be used for fraudulent purchases.

4.2.2.4 STAGE ACTIVITIES

Initiation can involve several different activities, ranging from target identification to the deployment of malware or similar tools to compromise a target. Generally, the activities can be grouped into three primary areas:

1. ***Preparation*** – This set of activities relates to the very first steps of the attack, where information is acquired, data is validated, or other preparatory actions necessary to perform the attack. A common aspect of preparation is the identification of a target individual or a target institution to exploit.
2. ***Delivery*** – This set of activities relates to the steps necessary to deploy and activate the attack or event. This could be the initial contact with the customer, initial contact with the institution, or the delivery of malware or other similar action to engage the target(s).
3. ***Initial Point of Compromise*** – Building on preparation and delivery, the initial point of compromise is that step that enables the economic crime to actually occur during execution. This activity could be acquiescence by the target, successfully logging into a target's account, or successfully initiating malware code.

4.2.2.5 STAGE ENTRY

The initiation stage is entered by an actor wanting to execute an economic crime attack or event.

4.2.2.6 STAGE EXIT

The initiation stage is exited, and transitioned to the next stage, through the initial engagement of a target.

4.2.3 EXECUTION STAGE

4.2.3.1 SUMMARY

To achieve the attack or event goals, and get to the point where an attacker can obtain some benefit, a serious of activities are necessary. It is in this stage that the attacker actually exploits a compromised account, utilizes a stolen credit card, or executes an unapproved transaction through malware.

Attackers approach this stage in many different manners, depending on their goals and the nature of the attack / event. Attackers typically have an established "playbook" they execute, which can be executed repeatedly when different accounts or attack pathways are established.

4.2.3.2 STAGE FOCUS

The execution phase is focused less on the target and more on the underlying attack pathway or mechanism to exploit. At this stage, the target is established and compromised.

4.2.3.3 EXAMPLES

In the context of an account takeover, the execution is a transaction on a compromised account, such as an unapproved or fraudulent transaction. Another example is convincing a compromised target to voluntarily perform a transfer or transaction.

4.2.3.4 STAGE ACTIVITIES

Execution can involve several different activities, ranging from physically initiating a fraudulent transaction to the exploitation of a compromised system or account holder. Generally, the activities can be grouped into two primary areas:

1. ***Exploitation*** – This set of activities involves the actions by the attacker to access or initiate the request tools or systems necessary to conduct the economic crime. This could be the attacker obtaining a verification code or authorization to perform transactions with an account.
2. ***Execution*** – This set of activities involves the core actions of the overall economic crime, and involves the attacker being in a position to directly or indirectly perform a fraudulent transaction or initiate the transfer of value away from another person or

entity. This could be the attacker gaining access to an online account system or adding another person's card to their digital wallet.

4.2.3.5 STAGE ENTRY

The execution stage is entered by an attacker successfully completing the initiation stage.

4.2.3.6 STAGE EXIT

The execution stage is exited, and transitioned to the next stage, through the attacker completing the steps to execute the fraud, and the transitions to the next stage, where the attacker obtains the value of the economic crime.

4.2.4 EXTRACTION STAGE

4.2.4.1 SUMMARY

Extraction is the final stage of the process, where the attacker obtains the results or financial benefits of the attack or event. In this context, extraction relates to the movement or transfer of monies or other similar assets out from the target to the attacker.

4.2.4.2 STAGE FOCUS

The extraction phase is focused on the attacker or malicious actor, and moves completely away from the target and mechanism of compromise. At this stage, the target has been compromised, the crime has been executed, and now the actor wants to complete the lifecycle by getting the money or value.

4.2.4.3 EXAMPLES

For example, in the context of the account takeover, extraction would be transferring money out of an account or obtaining an item or points obtained from a rewards program.

4.2.4.4 STAGE ACTIVITIES

Extraction can involve several different activities and, most importantly, can involve other systems, institutions, and even other targets or victims beyond the crime's target and method of compromise. Generally, the activities can be grouped into two primary areas:

1. ***Funds Transfer*** – This set of activities relates to the transactions or movement of funds, property, or the other value obtained form the crime away from the victim and the method of compromise to another location. This could be through a transaction with a collusive merchant, transfer money out of an account, or the transfer of property to another person.
2. ***Laundering*** – This set of activities relate to the actions taken by the actor to obfuscate, hide, or change the source of the value obtained through the crime into a form they

can control and use. This could be the withdrawal of cash from a financial institution, the sale of stolen property, or conversion of an asset from one form to another.

4.2.4.5 STAGE ENTRY

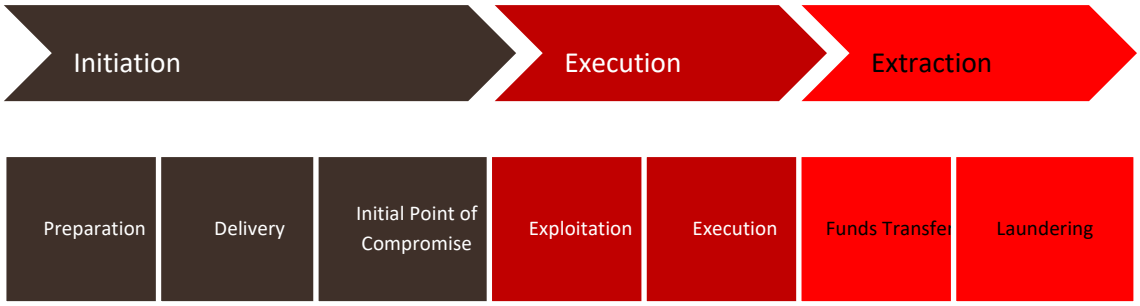
The extraction stage is entered by an attacker successfully completing, or executing, the attack or event.

4.2.4.6 STAGE EXIT

The extraction phase is exited, and the overall process completed, by the attacker moving funds or value obtained completely out of the control of the target and/or financial institution and placing the funds or value obtained within their sole control and use.

4.3 ASSEMBLY OF THE TYPOLOGY

Putting together all of the items from the above, we can visualize a typological structure that provides discrete sets of activities within a multi-stage process, enabling a detailed description of a specific economic crime while maintaining a level of flexibility that can be applied to most, if not all, economic crimes.



4.4 COMPLETING THE TYPOLOGY

With a topology structure in place, we can now extend each activity area of the typology by specifying the discrete activities and behaviors TTPs in industry parlance, that compromise the activity area. Further, we can strengthen the typology and make it more universally communicable through the standardization of activities, and their description, within a given activity area and limit additional situational or contextual information for a particular attack as embellishment on the standardized activity description.

Taking this approach also minimizes confusion and supports the process-driven approach inherent to attack chains. In dealing with complex economic crimes, the order, inputs/dependencies, results, scope, and much more of each activity within an activity area has critical significance, especially as controls are designed, implemented, and monitored. Reducing the creation of bespoke descriptions or attack chain structures; bespoke activity descriptions can reduce cross and inter-organization understanding, as terminology, structure, and discrete focus areas can widely vary team-by-team or organization-by-organization.

Additionally, this approach enables the creation of a catalogue for each of the activities. With a catalogue, stakeholders can reduce the time and effort necessary to create an attack chain. A catalogue also reduces the potential for duplicative or divergent attack chains descriptions.

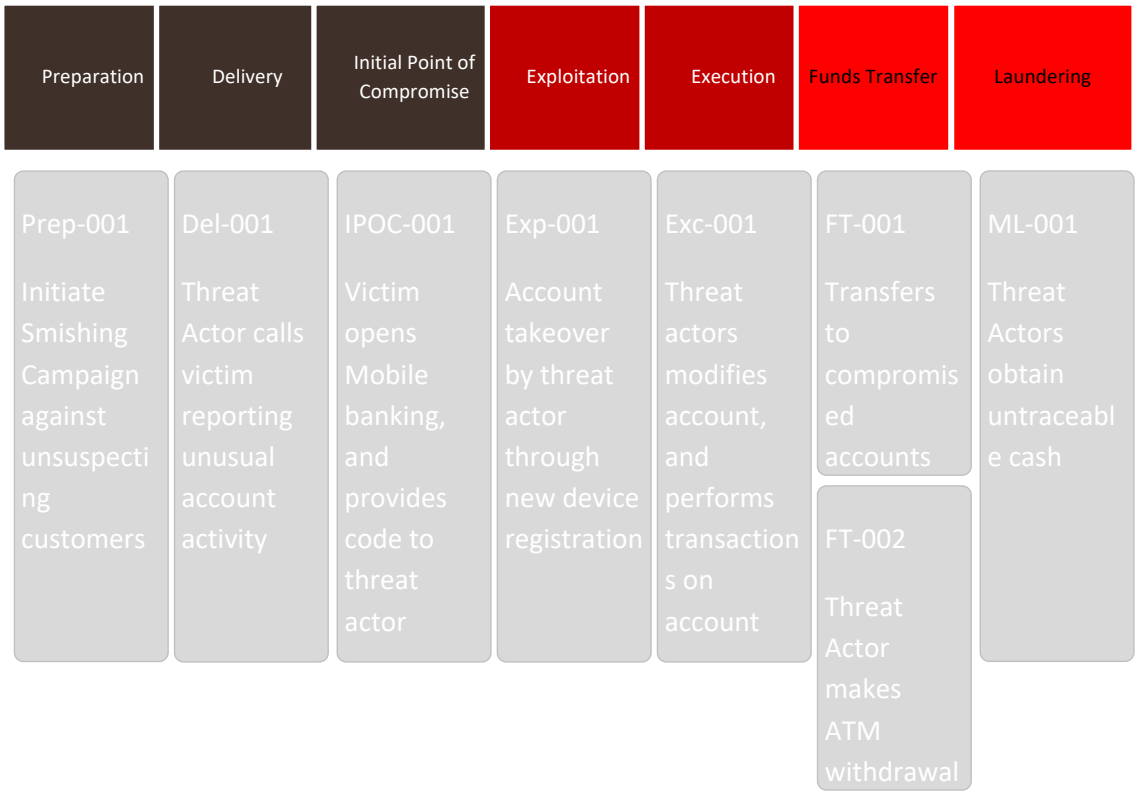
By standardizing and cataloguing the activities, the typology can be more readily communicated and understood between organizations, while enabling additional activities to be added over time to make the typology more robust and usable.

For example, downloading compromised information from a dark website is a recurring action that could be standardized as an activity within “Preparation” or “Delivery” activity Areas. We can catalogue this activity as “I-001 Dark Web Acquisition”, and embellish the standard description with useful particulars such as the dark web site, file name downloaded, threat team, and other useful factual information.

4.5 FULL TYPOLOGY USAGE EXAMPLE

The example below is an example of how the full typology can be used.

Attack Chain – #0000 – Mobile Banking Compromise



5 FRAMEWORK COMPONENTS

As we can see above, the typology provides a comprehensive view into the details of the attack chain. Even though the view is comprehensive, it is still missing useful context that can elevate the attack chain typology from an informational resource to a tool that can drive fraud prevention and disruption through improved detection and controls.

To create a more effective tool, additional information is necessary, such as the overall description of the attack or event, suggested approaches on how stakeholders can identify the attack, suggested approaches on how organization can prevent and mitigate the attack or event, and finally, what risk and control considerations are necessary.

With this additional information, we can achieve a full framework for describing, communicating, preventing, and disrupting economic crime activity.

5.1 FULL FRAMEWORK

The full Framework is comprised of 6 components:

5.1.1 ATTACK OR EVENT NAME AND ID

A reasonably descriptive and differentiating name of the attack, with a unique identification number for reference.

5.1.2 ATTACK OR EVENT SUMMARY

A brief summary description of the attack or event that can be quickly shared instead of the more complete description, below.

5.1.3 ATTACK OR EVENT DESCRIPTION

A detailed description of the attack or event.

5.1.4 ATTACK OR EVENT TOPOLOGY

The individual topological elements for each stage of the attack chain

5.1.5 IDENTIFICATION APPROACH

The processes and/or mechanisms that can be used to identify the attack, as early in the chain as possible.

5.1.6 PREVENTION & MITIGATION APPROACH

The actions that can be taken by an institution to deter, prevent, interdict, and mitigate the attack.

5.1.7 RISK & CONTROLS CONSIDERATIONS

Controls and/or tools that can be deployed to detect or identify, and manage the attack (or elements of the attack), at each stage of the attack chain.

5.2 FRAMEWORK EXAMPLE

Building on the example introduced above, here is the full framework together

Name and ID: Attack Chain – #0000 – Mobile Banking Compromise

Description: A customer is targeted by a threat actor, with the goal of compromising a customer's mobile banking account access. The customer is misled by the Threat Actor to provide security information, enabling the Actor to register a new device to the customer's account. Through the Threat Actor controlled device, the actor gains access and control of a customer's account, and expropriates customer's funds by transferring the funds to an external account or directly withdrawing the money.

Preparation	Delivery	Initial Point of Compromise	Exploitation	Execution	Funds Transfe	Laundering
Prep-001 Initiate Smishing Campaign against unsuspecting customers	Del-001 Threat Actor calls victim reporting unusual account activity	IPOC-001 Victim opens Mobile banking, and provides code to threat actor	Exp-001 Account takeover by threat actor through new device registration	Exc-001 Threat actors modifies account, and performs transactions on account	FT-001 Transfers to compromised accounts FT-002 Threat Actor makes ATM withdrawal	ML-001 Threat Actors obtain untraceable cash

Attack Typology:

Identification Approach: Utilize device and user fingerprinting methodologies to identify changes to the customer device while a customer's existing device continues to be utilized to access the account(s).

Prevention & Mitigation:

- Prevention – Educate customers through existing channels and within the mobile application to not share security information; Monitor for new devices and require

step-up / authentication for newly enrolled devices; Monitor the dark web / forums for campaign initiation by threat actors.

- Mitigation – Restrict new devices from performing certain account actions, such as customer information changes or fund transfers, for a reasonable period of time, e.g. 1 week. Maintain a list of compromised devices and threat actor indicators to prevent Threat devices to be utilized.

5.2.1 RISK & CONTROLS CONSIDERATIONS:

- Implementation of additional controls focused on device fingerprinting is dependent on a tool or solution that can analyze and track devices.
- Implementation of funds transfer and/or other account activities when a new device is registered must be carefully considered in the context of customer experience, and having controls in-place to implement such as capabilities.
- Account changes, such as phone or email, should already be closely monitored as those changes have an extremely common nexus with other account compromise, takeover, and fund expropriation attacks.

6 CHALLENGES / CONSIDERATIONS

6.1 ALTERNATIVES

- This is unique approach actively used by Barclays, a large, international FI; however, this structure and specific chain approach is not the only approach, there are other approaches in the marketplace.
- FS-ISAC, vendors, other FIs, and others in the marketplace have similar Attack Chain concepts that each contain a different perspective on elements involved in an attack
- For example, one chain may contain only 5 steps while another has 9 steps, one may not delve into the TTPs while another is only TTPs.
- Also, our approach was designed to balance expansiveness with thoroughness; other frameworks may focus only on Fraud events, or may focus on only one aspect of an attack such as focusing only customer behavior, and not emphasizing threat actor behavior.
- Ideally, the marketplace can harmonize around one approach / structure, which can foster cross-firm interfacing, while simultaneously co-operate with the other approaches used in more local circumstances

6.2 COMPATIBILITY

- In addition to inter-fraud chain connections, the framework is meant to be compatible with other frameworks, e.g. the MITRE ATT&CK or CDA frameworks.
- The overall conceptual and deeper elements of compatibility further foster understanding and a shared vocabulary across the landscape
- Compatibility, similar to alternatives above, does not mean that one framework is meant to replace another, it is meant to support integration and sharing of ideas and concepts between frameworks and the industry overall.

6.3 ADOPTION

- Critical elements to adoption are usability and accessibility.
- Inability to utilize the framework, and/or inability to participate in evolution of framework can reduce interest in adopting the framework
- To improve adoption, partnership and participation are critical
- To foster broader adoption, Barclays will partner and share with other entities in the Financial Service market, in addition to exploring partnerships in other business areas. Such as Technology, Medical, etc.

6.4 SYSTEM INTEGRATION

- In addition to cataloguing attack events, this framework can also facilitate the implementation of technology and operational controls related to attack events

- In order for this information to be integrated from a system standpoint, sufficient detail is necessary within the attack chain so that analytics, rule, and/or control teams can implement a new analytic / rule / control.
- As this framework evolves, one idea already under discussion is the inclusion of a sample detection rule or analytic, beyond just the technical description currently included.
- An offshoot of this is the investigation and evaluation of a standard rule structure or descriptor than be implemented to maximize usability by different systems / organizations.

6.5 TTP / IOC STANDARDIZATION

- One aspect of this framework is the inclusion of TTPs, including IOCs.
- TTP inclusion is critical to the framework, as it provides the lower-level detail needed to make the framework and its contents usable and actionable.
- IOC formats, such as STIX or YARA, might be too specific for efficient usage within the framework, but a standardized format could improve the adaptability and appropriability of the Attack chains

7 GLOSSARY

Term	Definition / Description
CyOps	Cyber Operations
JOC	Joint Operations Center
IM	Incident Management
RAIL	Rolling Action Item Log
SNOW	Service Now Ticketing Application
SIEM	Security Information and Event Management
IOC	Indicator of Compromise
TTP	Tactics, Techniques, and Procedures

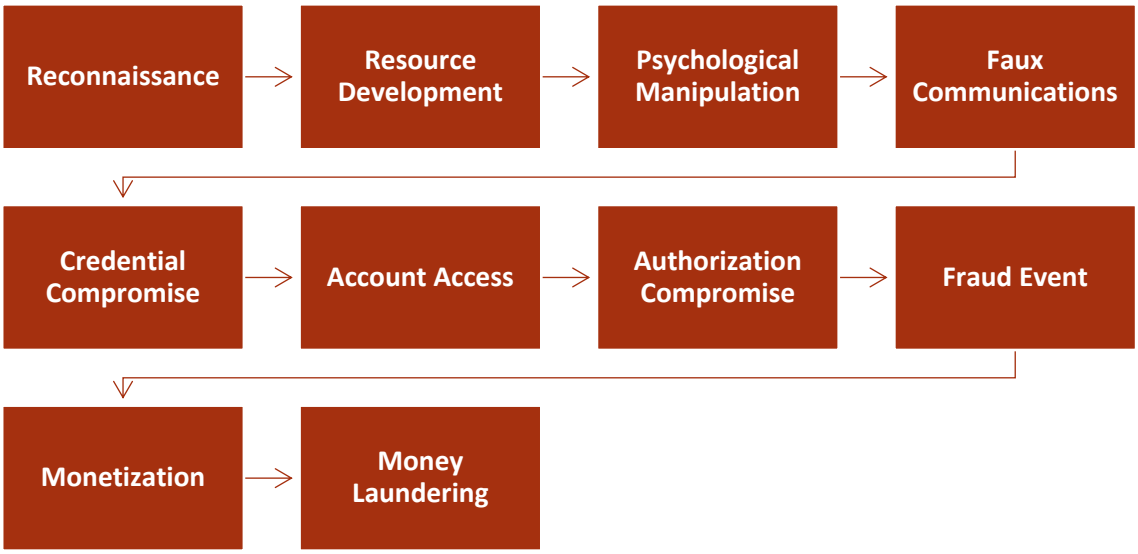
8 EVOLUTION

Operational Departments started using the Fraud Kill Chain to improve their Fraud Intelligence, Fraud Prevention and Fusion processes. This collaboration led to a series of modifications and updates. The process was iterative, allowing for continuous refinement. Through repeated evaluations and adjustments, the departments enhanced their tactics, techniques, and procedures. The version being published today represents the culmination of these improvements.

Bear in mind however, the following mantra:

No version of the Fraud Kill Chain is the Final version of the Fraud Kill Chain.

9 THE APRIL 2025 FRAUD KILL CHAIN



Reconnaissance	Resource Development	Psychological Manipulation	Faux Communications	Credential Compromise	Account Access	Authorization Compromise	Fraud Event	Monetization	Money Laundering
SMS Intercept	Acquire Infrastructure	Romance	Phishing	Keyloggers	Device Compromise	Location Spoofing	Victim Transfer	Cashout	Resale of Goods
Bots	Compromise Infrastructure	Impersonation	Spearphishing	Screen Capture	Insiders	Virtual Phone	Account Takeover	Subscriptions	Crypto Mixers
Malware	Social Networks Accounts	Accessibility Permissions	Smishing	SMS Intercept	Cloned Devices	Voice Changers	P2P Transfers	ATM Withdrawal	
Personal Info	Infected POS	Fake Loan Requests	Vishing	Card Dump Captures	Brute Force	Page Overlays	Imposter QR	Gift Cards	
Public Domain	Infected ATM	Loyalty Programs	Social Media	Session Cookie Capture	Session Hijack	Fake Extensions	NFC Payments	NFC Relay (Token Relay)	
Dark Web	SIP Services	Official Phone Number Spoofing	Message	HTTPS Intercept	Remote Access	2FA Compromise	Stolen Card Use	Crypto Purchase	
	Malvertising	Profitable Propositions	Scam Ads	Illegal Access to Database	Virtual Machines	Malware	Network Interception		
	App Repackaging	Employee Credentials	Fake Support	Password Stealer		Caller ID Spoofing	Mule Card Transfers		
	Malware	Employee Impersonation	Fake Call Centers	Phone Number Disclosure			Bonus Withdrawal		
	Supply Chain Compromise	Account Detail Changes	Fake (Merchant) Websites	Man in the Middle			ATM Jackpotting		
	Fake Accounts	Branded Resources	Fake Apps	Fake Forms			Shipping Redirect		
	Hosting Services	Website Redirects					Payments from Mule Account		
	Money Mules	Prepaid Reservations					Payment to Mule Account		
		Payment via Gift Card							
		Social Engineering							

9.1 RECONNAISSANCE

9.1.1 SMS INTERCEPT

9.1.2 BOTS

9.1.3 MALWARE

9.1.4 PERSONAL INFO

9.1.5 PUBLIC DOMAIN

9.1.6 DARK WEB

9.2 RESOURCE DEVELOPMENT

9.2.1 ACQUIRE INFRASTRUCTURE

9.2.2 COMPROMISE INFRASTRUCTURE

9.2.3 SOCIAL NETWORKS ACCOUNTS

9.2.4 INFECTED POS

9.2.5 INFECTED ATM

9.2.6 SIP SERVICES

9.2.7 MALVERTISING

9.2.8 APP REPACKAGING

9.2.9 MALWARE

9.2.10 SUPPLY CHAIN COMPROMISE

9.2.11 FAKE ACCOUNTS

9.2.12 HOSTING SERVICES

9.2.13 MONEY MULES

9.3 PSYCHOLOGICAL MANIPULATION

9.3.1 ROMANCE

9.3.2 IMPERSONATION

9.3.3 ACCESSIBILITY PERMISSIONS

9.3.4 FAKE LOAN REQUESTS

9.3.5 LOYALTY PROGRAMS

9.3.6 OFFICIAL PHONE NUMBER SPOOFING

9.3.7 PROFITABLE PROPOSITIONS

9.3.8 EMPLOYEE CREDENTIALS

9.3.9 EMPLOYEE IMPERSONATION

9.3.10 ACCOUNT DETAIL CHANGES

9.3.11 BRANDED RESOURCES

9.3.12 WEBSITE REDIRECTS

9.3.13 PREPAID RESERVATIONS

9.3.14 PAYMENT VIA GIFT CARD

9.3.15 SOCIAL ENGINEERING

9.4 FAUX COMMUNICATIONS

9.4.1 PHISHING

9.4.2 SPEARPHISHING

9.4.3 SMISHING

9.4.4 VISHING

9.4.5 SOCIAL MEDIA

9.4.6 MESSAGE

9.4.7 SCAM ADS

9.4.8 FAKE SUPPORT

9.4.9 FAKE CALL CENTERS

9.4.10 FAKE (MERCHANT) WEBSITES

9.4.11 FAKE APPS

9.5 CREDENTIAL COMPROMISE

9.5.1 KEYLOGGERS

9.5.2 SCREEN CAPTURE

9.5.3 SMS INTERCEPT

9.5.4 CARD DUMP CAPTURES

9.5.5 SESSION COOKIE CAPTURE

9.5.6 HTTPS INTERCEPT

9.5.7 ILLEGAL ACCESS TO DATABASE

9.5.8 PASSWORD STEALER

9.5.9 PHONE NUMBER DISCLOSURE

9.5.10 MAN IN THE MIDDLE

9.5.11 FAKE FORMS

9.6 ACCOUNT ACCESS

9.6.1 DEVICE COMPROMISE

9.6.2 INSIDERS

9.6.3 CLONED DEVICES

9.6.4 BRUTE FORCE

9.6.5 SESSION HIJACK

9.6.6 REMOTE ACCESS

9.6.7 VIRTUAL MACHINES

9.7 AUTHORIZATION COMPROMISE

9.7.1 LOCATION SPOOFING

9.7.2 VIRTUAL PHONE

9.7.3 VOICE CHANGERS

9.7.4 PAGE OVERLAYS

9.7.5 FAKE EXTENSIONS

9.7.6 2FA COMPROMISE

9.7.7 MALWARE

9.7.8 CALLER ID SPOOFING

9.8 FRAUD EVENT

9.8.1 VICTIM TRANSFER

9.8.2 ACCOUNT TAKEOVER

9.8.3 P2P TRANSFERS

9.8.4 IMPOSTER QR

9.8.5 NFC PAYMENTS

9.8.6 STOLEN CARD USE

9.8.7 NETWORK INTERCEPTION

9.8.8 MULE CARD TRANSFERS

9.8.9 BONUS WITHDRAWAL

9.8.10 ATM JACKPOTTING

9.8.11 SHIPPING REDIRECT

9.8.12 PAYMENTS FROM MULE ACCOUNT

9.8.13 PAYMENT TO MULE ACCOUNT

9.9 MONETIZATION

9.9.1 CASHOUT

9.9.2 SUBSCRIPTIONS

9.9.3 ATM WITHDRAWAL

9.9.4 GIFT CARDS

9.9.5 NFC RELAY (TOKEN RELAY)

9.9.6 CRYPTO PURCHASE

9.10 MONEY LAUNDERING

9.10.1 RESALE OF GOODS

9.10.2 CRYPTO MIXERS