Leveling Up: A Cyber Fraud Prevention Framework for Financial Services

A publication of the FS-ISAC Cyber Fraud Prevention Framework Working Group

Leveling Up: A Cyber Fraud Prevention Framework

Contents

Leveling Up: A Cyber Fraud Prevention Framework

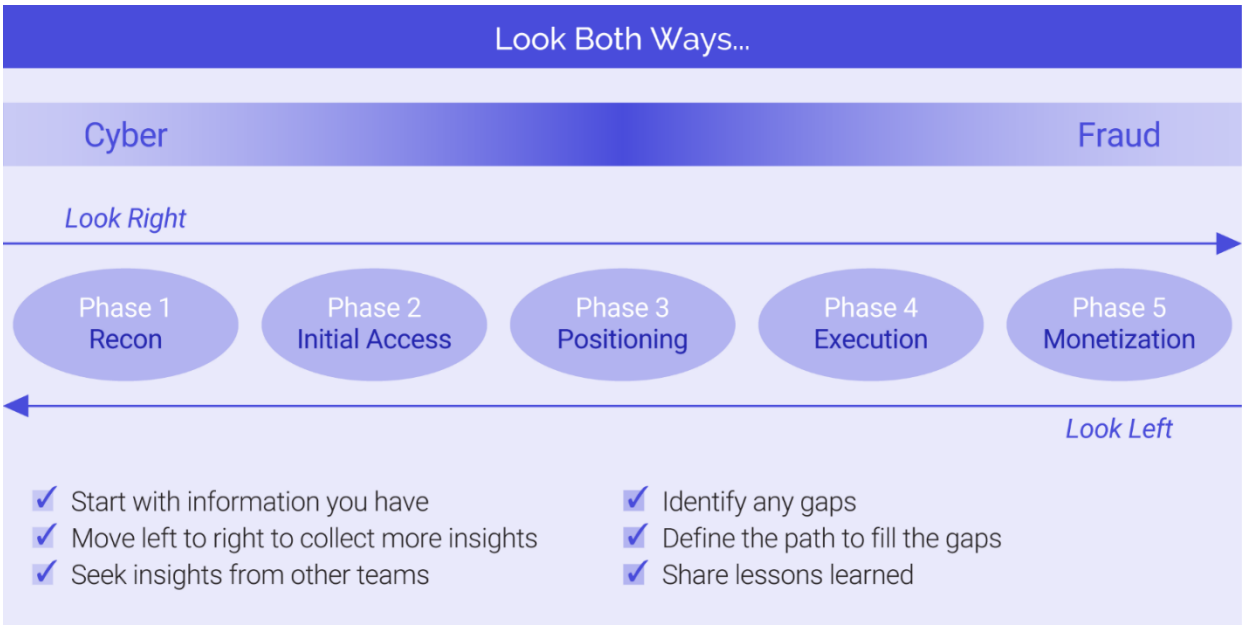
Executive Summary

Preventing fraud is a constant challenge in the financial services sector. To succeed, an institution requires data, intelligence, and specific capabilities — all of which may be siloed in cybersecurity, fraud, financial crimes/anti-money laundering, and other teams.

To help such teams coordinate and direct their fraud-fighting efforts, FS-ISAC's Cyber Fraud Prevention Framework Working Group developed a method to de-silo information to help teams pool information regarding cyber fraud — i.e., frauds conducted on cyber channels. This Cyber Fraud Prevention Framework is designed to coordinate and maximize financial institutions' data and capabilities specific to the financial services sector. Key aspects of the Framework include its:

- Common structure and lexicon to help teams identify their knowledge gaps
- Protocol for partnership on fraud response
- Method for sharing indicators and lessons learned with the financial sector

A primary advantage of implementing the Cyber Fraud Prevention Framework is that it accelerates the information-gathering process. Teams are guided to start with whatever information they have specific to the phase of the fraud they discover, identify activity from other phases, and seek additional information from colleagues — to look both ways, in sum. This structured process fills in the blanks of the fraud so that controls can be implemented sooner, and it helps prevent successful frauds in the future.



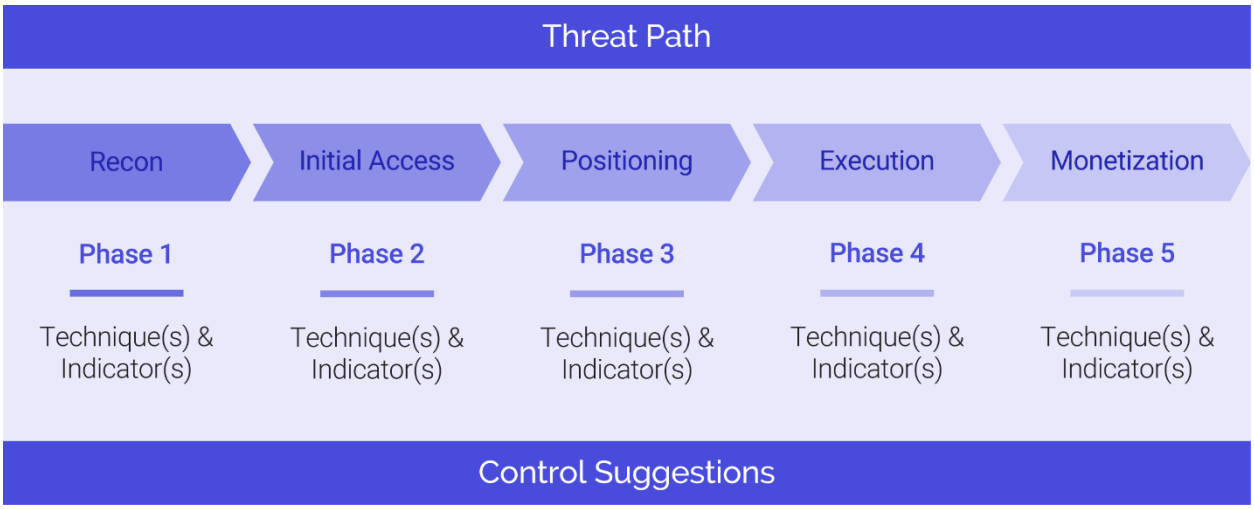
A second, equally important aspect of the Framework is that it formalizes and facilitates information sharing in the sector. Threat actors typically attack multiple targets at once or in close succession. Sector-level awareness helps firms introduce fraud controls that prevent further impact.

More and more, the financial services sector recognizes that the cooperation of fraud analysts, cybersecurity staff, financial crime investigators, and intelligence-sharing groups fosters more effective collaboration and greater cost efficiency within institutions. Those are worthy achievements for any firm. But sharing actionable fraud intelligence with the entire sector helps achieve the most important goal of fraud prevention: Safeguarding reputations, financial assets, and trust in the sector.

Overview of the Cyber Fraud Prevention Framework

The Cyber Fraud Prevention Framework builds on and extends familiar cyber frameworks, but it's built for financial services institutions, where threat events can take many different forms, involve multiple participants, and touch several systems and processes. For that reason — and despite a nearly endless potential combination of fraud elements — the Cyber Fraud Prevention Framework structures fraud in five phases.

The order of the five phases describes the lifecycle of attacks conducted through a cyber channel that includes potential or actual fraud monetization. Teams are guided to list the techniques and indicators they've discovered in each phase, as well as the controls associated with mitigation. As such, the Framework and its components provide detail around a threat path while offering a level of flexibility that can be applied to most, if not all, attack scenarios.



Each phase is associated with specific adversarial attributes and actions.

Phase 1 — Recon: The threat actor's passive or active actions to determine their target, collect information, set up infrastructure, and plan for attempted fraud. Recon ends at the entry point into the attack.

Phase 2 — Initial Access: The threat actor's actions to gain an initial foothold for fraud against a consumer, financial services institution, or other entity (e.g. third-party vendor or a vendor's sub-service provider).

Phase 3 — Positioning: The threat actor's attempts to change and/or collect account information that will be forwarded to the controlled infrastructure.

Phase 4 — Execution: Process that converts stolen data to money, typically executed within business procedures that send fraudulent/unauthorized funds to the threat actor.

Phase 5 —Monetization: The method of payment in which stolen funds are transferred to the threat actor.

This five-phase concept can be applied to a wide range of scenarios, from application fraud and account takeover to economic crimes like money laundering and sanctions avoidance.

Cyber Fraud Prevention Framework Workbook

FS-ISAC members can access the Cyber Fraud Prevention Framework workbook, resources, and updates via the Public Connect Channel. PowerPoint slides are also freely available to FS-ISAC members as a tool to inform and guide colleagues and stakeholders.

Information about FS-ISAC membership is available here.

The Framework in Practice

Step 1. Assemble the teams

An institution can put the Framework into action as soon as it detects a threat. The first step is to assemble representatives from all the teams involved in cyber fraud prevention — cybersecurity, threat intelligence, financial crimes/AML, data analytics, fraud, etc.

Step 2. Start with what you have

Next, each team should research the techniques and indicators they've discovered and bring their initial research to the collective table for full analysis. That way, everything that is known about the fraud can be surfaced.

Fraud indicators can be discovered at any phase of an attack, so the Framework is designed to be implemented wherever the indicator is found. Each phase can contain a mix of discrete adversarial techniques and indicators. The table below shows an example of an account takeover initiated through a call center, illustrating techniques that threat actors are known to use in each phase.

Account Takeover – Call Center (Phone)				
Phase 1 **Recon**	Phase 2 **Initial Access**	Phase 3 **Positioning**	Phase 4 **Execution**	Phase 5 **Monetization**
Dark web marketplace	Call center social engineering	Account linking	Request loan	Electronic funds transfer/automatic clearing house
Elder abuse	Member impersonation	Add authorized user	Request rollover distribution	Check
Family fraud	Phone port-out	Add beneficiary	Request regarding fictitious emergency	Digital payments
Identity theft	SIM swap	Change account details	Retirement plan disbursement	
Insider threat	Spoofed phone number	Change notification settings	Submission of fictitious claim	
IVR processing		Collect personal information		
Mail theft		Create persistent access		
Malware infection		Mobile wallet provisioning		
Open-source intelligence		New payee		
Third-party data breach		Request execution forms		
Social engineering				
Social media research				

Cyber Fraud Prevention Framework Techniques

The Framework contains over 200 techniques to help the teams review and uncover the full threat path used by the threat actor.

The teams will likely bring perspectives unique to their field in the various phases. For example, cybersecurity teams tend to have the most knowledge about Phase 1 (Recon) and Phase 2 (Initial Access) and can bring insights on domain registration, IP intelligence, and reviews of social media, the dark web, and digital fingerprints, among other issues. Similarly, fraud teams can share their perspectives on account activity, data analysis, and risk rule alerts. Treasury management or anti-money laundering (AML) functions may have insight on call center alerts and indicators, among other issues. Sometimes perspectives overlap, such as cybersecurity and fraud teams' insights on Phase 3 (Positioning).

When those techniques are discovered, the specific details and indicators should be documented in terms standardized across the institution (appointing someone to manage full documentation may help).

That process:

- Limits irrelevant situational or contextual information
- Facilitates accurate, comprehensive communication of the fraud lifecycle
- Directs team members toward aspects of the scheme unique to their domain

Step 3. Look left

Having identified as much as they know on a team level, the group uses the collated information to uncover how the criminal achieved that phase — they "look left" on the Framework. The collective insights of the group highlight gaps in information that direct them to gather more, as yet unknown, data. (It should be noted that all members of FS-ISAC have access to threat feeds and member intelligence.)

Step 4. Place the controls

By walking through the crime, the group can gather insights into the fraud, identify indicators, and place controls to prevent the criminal from moving forward. Those insights can be used to analyze other accounts and transactions for similar fraudulent activity.

Importantly, if the group continues to "look left" and pools information, it will develop a clearer understanding of fraud activity in the institution. If the group uses that knowledge to "look right," participants can better predict how that activity will proceed (or has already proceeded). That information can be used to detect or prevent other threats.

Note that beyond identifying elements and data indicative of fraud to disrupt and prevent ongoing activity, the Framework also promotes alerting on outliers, i.e., data that deviates from tolerances around a baseline.

Treasury Management Case Study: Looking Left to End a Fraud

Client Accounts Under Attack

In this banking institution, fraud teams observed a spike in Treasury Management account takeover (ATO) attacks — as many as 10 a day. Each successful ATO caused six- to seven-figure client losses. The fraud team began to suspect cybercriminals had developed a complex new cyber fraud attack method.

By reviewing the compromised accounts, the fraud team discovered the attack's Phase 3 (Positioning), Phase 4 (Execution), and Phase 5 (Monetization) techniques and that the cybercriminals were adding authorized users, changing account info, withdrawing funds, and transferring stolen money, ultimately leading to fraudulent wires to money mule accounts at other banks (money mules are people who permit their accounts to be used by criminals to launder money). But fraud teams had limited insight into the cybercriminals' Phase 1 (Recon) and Phase 2 (Initial Access) tactics, though some clients reported a vishing event where the cybercriminal already appeared to have access to their accounts.

So fraud contacted cybersecurity and together, they started with what they knew.

Solving the Mystery with the Cyber Fraud Prevention Framework

The Framework gave the cybersecurity team a list of possible Phase 1 (Recon) and Phase 2 (Initial Access) tactics. With that, the group "looked left" and asked:

- Are cybercriminals conducting malware infections on client systems?
- Have they recruited an insider or compromised a third party?
- Do these ATOs involve spear-phishing emails, smishing (phishing), or credential-stuffing attacks?

The cybersecurity team reviewed cyber controls, internal logs, threat intel reporting, and peer shares to map the complex attack to the Framework. There was no evidence of insider involvement, compromised third parties, compromised client lists, or unmitigated credential-stuffing attacks. It became clear that a broadly targeted phishing event caused a spike in highly targeted impersonation vishing attacks. Then evidence of malvertising and SEO poisoning became apparent.

A Common Understanding to Mitigate the Attack

Cybersecurity could now begin to fill in the Framework's blanks regarding tactics from Phase 1 (Recon) and Phase 2 (Initial Access). Leadership was able to see how the attack worked by viewing the full lifecycle and gaining a common understanding of the threat the firm faced. That helped to clarify operational priorities to mitigate the cybercriminal's tactics.

Cybersecurity teams could then report changing cybercriminal tactics in real time and create feedback loops with fraud teams. These feedback loops repeatedly demonstrated that search engine malvertising directly led to a spike in ATOs.

While the cybersecurity team took down phishing domains and traced vishing calls, the key to mitigating the attack was stopping the search engine malvertisements, i.e., online ads that download malware when people click on them. The Framework's mapping tied Treasury Management losses to specific search engine ads, which prompted a closer business relationship with the search engine companies and an adjusted allocation of marketing budget to counter the cybercriminals.

In the end, investments to mitigate malvertising led to eight months without a successful ATO by the cybercriminal group.

Treasury Management Case Study — Threat Path				
Phase 1 Recon	**Phase 2 Initial Access**	**Phase 3 Positioning**	**Phase 4 Execution**	**Phase 5 Monetization**
Create domain/email infrastructure	Social engineering	Add authorized user	Bank account withdrawal	Bank transfer
Open-source intel	Vishing account holder	Change account information (email, username, phone, address, account password)	Bank transfer	Wire
Spoofing				

Strategic Applications of the Framework

Existing cyber-focused frameworks commonly have a single tactic for "financial theft," which overly simplifies a wide variety of financially motivated threat actors with dissimilar tactics and levels of sophistication. Mapping to this Framework can help distinguish cybercriminal groups by their tactics and determine how to prioritize spending on controls. The Framework also helps standardize how cybercriminal threats are described and helps the sector work collaboratively to prevent fraud.

In effect, using the Framework develops a topology of fraudulent activity. That information can be used strategically, both internally and externally.

- Internally, the information can be used to design countermeasures and controls.
    - If budget and planning are required to implement the controls, determine who else could have been involved in the discussion and how the Framework can be used in other scenarios.
    - Consider mapping critical scenarios and look for patterns in techniques that may point to unknown knowledge gaps.
- Externally, the key pieces of intelligence, including indicators of fraud and techniques, can be assembled and shared with the sector to prevent criminals from successfully attacking other financial institutions and undermining trust in the sector.

Using the Framework is a process — and potentially a culture shift — that will take time to establish. However, it helps participants understand the needs of the wider organization and streamline future investigations. It also creates a shared language to better describe and categorize threats. Used properly, the Framework will create efficiencies, preserve revenue, and maintain consumers' trust in the institution and the sector.

Potential Outcomes of Financial Services Sector Collaboration

It's expected that over time, the Framework will facilitate the creation of a sector-wide library of threat paths. This common taxonomy will reduce the time and effort necessary to design threat paths for every fraud attempt, prevent duplicative or divergent techniques and descriptions, and enhance tagging and metrics across the sector. That could lead to greater accuracy in collated threats and metrics. Thus, sharing actionable fraud threat intelligence provides a better view of the threats we all face.

It opens a more holistic view as well, as evidenced by the FS-ISAC Cyber Fraud Prevention Framework Working Group. The group first viewed the techniques threat actors utilize in each phase of the lifecycle from the perspective of an insurance provider. As FS-ISAC members from banks, credit unions, and investment firms joined the Working Group, it quickly grew to over 300 members and the aperture on fraud widened.

The collaboration showed that each subsector sees a narrow portion of the lifecycle of a threat. For example, insurance may see fraud through the lens of a fraudulent claim or redirected payment, but a new aspect of the threat is revealed when that financial activity passes through a bank or credit union. The more information collected, the broader the view became. This magnifies the great benefit already gained by a broader internal view and opens the door for a true 360-degree view of a threat.

Future of the Framework: Governance, Adaptations, Controls, and Heat Mapping

Governance: The design and structure of the Framework is not immutable. The Framework is designed to respond to a wide variety of threats and scenarios and fulfill a critical need in the sector. Ideally, financial institutions, vendors, subject matter experts, and other stakeholders will contribute ideas and participate in the evolution of the Framework. FS-ISAC will act as a steward for the Framework, lending expertise and perspective in its governance and management.

Extensions/adaptations: The Cyber Fraud Prevention Framework is a living document created collaboratively by contributions from multiple financial institutions. As a result, the Framework is meant to be widely relevant and used by any financial institution.

This Framework can be used as a foundation for other topologies that capture and document cyber, fraud, and economic crime events. Ultimately, it gives the industry an opportunity to introduce standardized definitions and descriptions, facilitating new creations while maintaining compatibility and adaptability with the core Framework.

Control suggestions: In support of better industry responsiveness, the Framework could incorporate control suggestions for each threat path, representing the actions an organization could take to deter, prevent, interdict, or mitigate the attack through tools or operational processes.

Control suggestions are highly dependent on the nature of the threat, and the various behaviors and techniques in the threat path. Nonetheless, they could enable an organization to quickly check its systems and tools to determine if they are appropriately positioned to protect the institution, its consumers, and its stakeholders.

Heat mapping: Patterns quickly emerge when the Frameworks of multiple fraud scenarios are shared and merged. A feedback tool will be developed for members to share their threat paths to be collated and analyzed through heat mapping to pinpoint key exploitation techniques, standard monetization methods, and areas where additional awareness and controls would benefit firms.

Conclusion

Fraud attempts are increasing and the losses — financial and reputational — are mounting. Halting the fraud lifecycle as it unfolds is crucial for financial services institutions and a key focus of FS-ISAC and many of its member institutions.

We believe that the Framework developed by the FS-ISAC Cyber Fraud Prevention Working Group may be an exceptionally effective solution. By looking left and right, firms can see the lifecycle of an active fraud. Capitalizing on the discrete knowledge and specialized skills of teams provides the means to disrupt threat actors. Inserting the right controls in the right place can prevent that fraud from occurring again.

The impact at the firm level can be substantial — using the Framework saved one bank hundreds of thousands of dollars a day, as the case study shows. Compound that across the sector, and the ROI on the Framework could be extreme.

One way to increase the ROI is to share the results of the Framework with peers. That will publicize threat actors' tactics and techniques in each phase of an attack, helping other institutions prevent fraud too. In time, whether we look left or right, the entire sector will see fewer and fewer frauds.

For media inquiries, email media@fsisac.com. The FS-ISAC Cyber Fraud Prevention Framework Working Group can be contacted for inquiries, feedback, and enhancement requests at cfpf@fsisac.com. To join the Cyber Fraud Prevention Framework Working Group, FS-ISAC members can refer to the COI Experience in the Member Services app.

FS-ISAC members can access the workbook, resources, and updates related to the Cyber Fraud Prevention Framework via the Public Connect Channel.

Appendix

The use of industry frameworks and their associated development and deployment has grown over the past few decades across multiple industries. Frameworks provide a structured mechanism to document and organize the factors and associated details for a specific process.

Cybersecurity frameworks typically shift defense and investigation teams' focus to the indicators of compromise that alert firms to intrusion and classify, categorize, map out, and disrupt the tactics, techniques, and procedures (TTPs) attackers use. These cyber frameworks have delivered a demonstrable and positive impact on cybersecurity in financial services and have improved detection capabilities and responsiveness to attacks.

Well-known and commonly used cybersecurity frameworks include:

- Cyber Kill Chain: Lockheed Martin's seven-step model that lists the phases and TTPs of an exploit
- MITRE ATT&CK®: The MITRE organization's compilation of observed adversarial TTPs that has been incorporated in many threat models and methodologies
- Diamond Model of Intrusion Analysis: The US Department of Defense model that helps identify adversaries and their infrastructure, capabilities, and targets

As the Cyber Fraud Prevention Framework becomes customary, it will increasingly minimize confusion and support the process-driven approach inherent to attack chains by standardizing attack structures and elements. Reducing bespoke attack chain models or structures can improve cross- and inter-sector understanding and eliminate variances in terminology, structure, and focus areas that can vary between teams.

Further, by standardizing and cataloging the activities, the typology can be more readily communicated and understood among financial services firms. Additional activities can be added over time to make the Framework more robust and usable in the sector.