SLK
an Altimetrik company

WHITEPAPER

FraudOps for Mitigating Banking Frauds

www.slksoftware.com

Contents

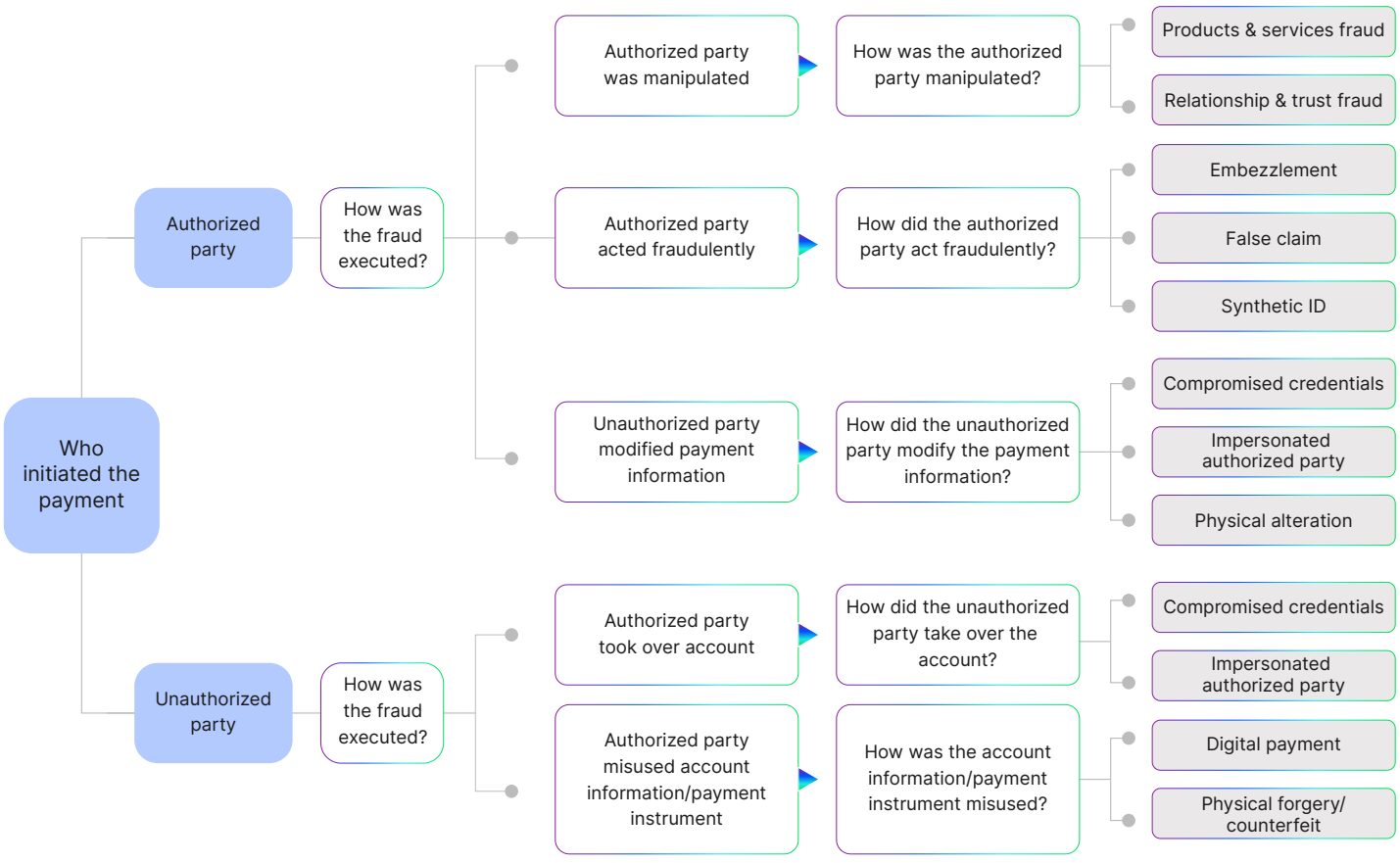
Frauds in Flux: Adapting to New Avenues in the Banking Realm

Financial frauds are criminal activities that function parallelly with financial systems worldwide. Banking has been one of the primary targets of financial frauds, utilizing loopholes in processes, systems, technologies, and policies, as well as a lack of consumer awareness. As the banking industry evolves with time and technology, fraudulent activities have evolved with new methods and schemes.

Frauds cause banks and their customers billions of dollars in losses and recovery. Fraudulent activities also change with changing demand for certain services and banking products. For example, during the pandemic and lockdowns, identity theft almost doubled in 2020 compared to 2019 through imposters claiming to provide government (relief) services during the crisis, helping them gather sensitive banking data from consumers (fool.com). On the other hand, credit card fraud saw a minor decline due to the restricted commercial activities at the time. The bigger problem arises from the increasing cost of fraud prevention, mitigation, and recovery. The Global Banking Fraud Index 2023 by SEON reported that US financial institutions bear around $4.23 in total costs for every dollar of fraud, a 4.2% increase in 2022. Thus, banking institutions need to prevent and mitigate fraud cost-effectively. But before such a strategy can be implemented, it is important to understand the types of banking frauds and the vulnerabilities they exploit.

Types of Banking Frauds

Banking fraud can be classified into a few broad categories depending on the source or nature of the fraudulent activity. For instance, fraudsters can be classified into people with direct and indirect access to banking services and data. Understanding the source of vulnerabilities is important to implement strict mitigation strategies.



Source: FraudClassifier

That said, here are a few of the most common types of banking frauds affecting banks and their customers.

Account Takeover:

When fraudsters take over the account by acquiring IDs and passwords to bank accounts. The United States Federal Trade Commission reported $5.8 Bn lost to frauds in 2021, a 70% rise from the previous year. Account takeover is a broad category that includes phishing, credential stuffing or bot attacks, social engineering scams, cybersecurity vulnerabilities, and call center fraud.

New Account Fraud:

One of the most common types of fraud, new accounts are used by fraudsters to utilize loopholes in policies or services like instant access to capital on cheque deposits. Fraud identities, also called mules, often use stolen credentials to create accounts and channel money to other sources using the account. People have also tried original identities to commit these kinds of frauds, but they are significantly lower and easier to mitigate or recover.

Payment Frauds:

It is a broad category of fraudulent activities that utilize the lack of awareness, education, or the general innocence of consumers. Consumers are manipulated to initiate transactions to fake accounts, services, businesses, charities, or other scams, which are then quickly moved to other accounts in complex and untraceable ways.

ACH Frauds:

One of the most critical forms of fraud, hackers utilize vulnerabilities in Automated Clearing House (ACH) systems implemented by authorities. They intercept transactions and redirect them to non-target accounts, leaving banks and authorities to investigate the transactions and costing valuable resources apart from the losses.

Cheque Frauds:

This is a common type of fraud that has declined over the years due to the declining use of cheques in banking services. However, it remains a threat to consumers and has been used to commit fraud. It includes using paper-based payment methods like cheques, wire transfers, money orders, etc. Cheques and wire transfers still remain the most impacted payment methods for fraudulent activities at 66% and 39%, respectively (2023 AFP Payments Fraud and Control Survey).

Card Frauds:

Another prevalent form of fraud, stolen card information can be easily used to make unauthorized transfers and payments. Fraudsters utilize the difference in jurisdiction and policies in cross-border payments to remain untraceable and protected from incrimination.

Application Fraud:

Another use of stolen credentials, fraudsters use these stolen identities to open new accounts, establish credit lines, and/or apply for loans. They often remain undetected until the first repayments are due and remain unfulfilled. These cause direct losses to banks instead of scamming through consumers.

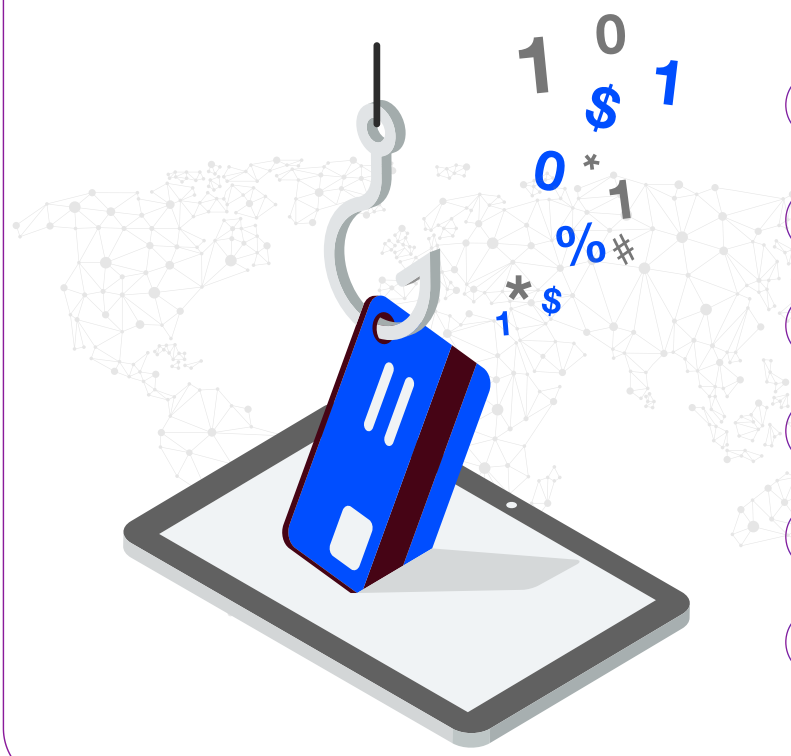
These frauds are still categorized broadly through banking services and activities. Identity theft is the most common method of accessing banking services for fraudulent activities, and the lack of consumer awareness is the most commonly exploited loophole for fraud.

However, frauds also utilize other flaws in the banking system in combination with ID theft and consumer manipulation to commit these crimes. Let's look at banking services that bring vulnerabilities to the system.

Banking Services, Technologies, and Policies Vulnerable to Frauds

Banking employs a host of services and technologies to serve its customers. While banks enable strict security measures to prevent fraud, they do not consider human and non-technical factors. Here are some of the most affected banking services and systems by fraud.

6 Ways how to avoid credit card fraud



1. Weak Password Policies and Authentication Processes
2. Customer Due Diligence
3. Inadequate Card Security Measures and Transaction Monitoring
4. Open Banking and Third-Party Risks
5. ATM and Point of Sale Skimming
6. Insider Frauds

1 Weak Password Policies and Authentication Processes

Access to banking and financial services is secured mainly through customer-generated passwords and authentication processes. Weaknesses in either of these result in account takeovers and other scams, leaving accounts vulnerable to various forms of fraud.

2 Customer Due Diligence

Many banking services require minimal documentation and authentication of customer IDs. This is especially true for existing and recurring customers. It leaves banks vulnerable to fake accounts and related fraud.

3 Inadequate Card Security Measures and Transaction Monitoring

Card jacking is among the most common banking frauds due to these inadequacies in card security. Banks also handle large volumes of transactions daily, making monitoring and flag suspicious activities very difficult. Seasoned fraudsters also employ tactics to evade such flagging systems if and when they are put in place.

4 Open Banking and Third-Party Risks

With the advent of API-based connectivity for banking services, third-party systems and banking integrations open vulnerabilities that hackers can exploit to hijack transactions or breach databases.

5 ATM and Point of Sale Skimming

Fraudsters can use unmonitored ATMs and point-of-sales to capture customer account data. This data is then used to steal identities and carry out fraudulent activities masked under the name of real customers.

6 Insider Frauds

One of the most disruptive methods of banking fraud; data leaks from people within the banking organizations can cause significant harm to the business. Data breaches are limited to the database exposed during a hack, but data leaks can be much more extensive and disruptive. It is also much more challenging to identify and prevent than other frauds if the people involved have the right knowledge and expertise.

Apart from these vulnerabilities, banking frauds can also utilize loopholes in compliance and regulatory mechanisms in the banking IT infrastructures to gain access to data. There are many other ways, like social engineering scams, where banking systems are not utilized directly for fraudulent activities.

Customer (lack of) awareness and education remains a major roadblock to preventing banking fraud and is a more significant challenge for banks due to the millions of customers in most banks' portfolios.

SLK has established its highly specialized center of excellence (CoE) for FraudOps to provide banks with the necessary skills, systems, processes, and other improvements to prevent frauds cost-effectively. We use a business-centric approach to provide banks with state-of-the-art fraud prevention, investigation, and recovery services. Here's a brief overview of the SLK's offerings.

SLK's FraudOps Center of Excellence

Our FraudOps CoE is established on business-centric and result-oriented approaches. We take a bank's processes, available skills and technology for FraudOps and establish a better line of defense by filling in the gaps and empowering them for accuracy. The framework that enables these capabilities is designed on the following principles.

Resource Analysis

SLK conducts an extensive analysis of the current skills and resources in the banking environment. These resources are mapped to skills and competencies to identify gaps that require attention. We help banks fill these gaps as the process moves forward.

Based on the assessed and mapped skills, and the nature of business, our CoE sets the knowledge foundation to build a resilient and reliable process for FraudOps.

Process and Control

This step considers several factors to establish better control over all the processes involved in FraudOps:

- Upstream and downstream processes are thoroughly studied, assessed and mapped, focusing on standardizing them
- Legal and regulatory compliances are also reviewed to define risks and account for them during process redesign
- Failure mode and effect analysis is performed for holistic optimization and risk mitigation

This helps us build controls for governance, benchmarking, and performance, enabling the CoE to transition to a steady state.

Industry Trends and Technology

As controls are established through standardization and optimization, CoE provides the client with fraud trends and studies and recommendations to incorporate changes in operations, processes and procedures. In parallel with process transformation, AI and RPA are implemented to gain higher efficiency and accuracy and, wherever possible, bridge the gaps.

Depending on the analysis and studies, SLK's FraudOps CoE utilizes various methodologies to improve and optimize the processes with measurable metrics and SLAs. Our comprehensive and inclusive solutioning delivers operational transformation, technology-enabled advantages, and a broad range of human capital training, development, and certifications.

About Us

SLK is a global technology services provider focused on bringing AI, intelligent automation, and analytics together to create leading-edge technology solutions for our customers through a culture of partnership, led by an evolutionary mindset. For over 20 years, we've helped organizations across diverse industries - insurance providers, financial service organizations, investment management companies, and manufacturers - reimagine their business and solve their present and future needs. Being A Great Place To Work Certified, we encourage an approach of constructively challenging the status quo in all that we do to enable peak business performance for our customers and for ourselves, through disruptive technologies, applied innovation, and purposeful automation. Find out how we help leading organizations reimagine their business at https://www.slksoftware.com/