SCTE•ISBE CABLE-TEC EXPO® 2020
VIRTUAL EXPERIENCE » OCTOBER 12-15

2020 Fall Technical Forum
SCTE·ISBE • NCTA • CABLELABS®

A Taxonomy of Fraud Experienced by Network Service Providers

So Many Ways People Try to Take Others' Money!

A Technical Paper prepared for SCTE•ISBE by

Kevin Taylor
Fellow
Comcast
Englewood, CO
Kevin_Taylor2@comcast.com

Steve Goeringer
Distinguished Technologist
CableLabs
Louisville, CO
s.goeringer@cablelabs.com

Eric Winter
Assistant Vice President Investigations and Technical Risk
Cox Communications
Atlanta, GA
Eric.Winter@coxinc.com

Michael Khalilian
Senior Director
Comcast
Philadelphia, PA
Michael_Khalilian@comcast.com

Table of Contents

Title **Page Number**

List of Figures

Title **Page Number**

1. Introduction

All service providers and retail businesses experience crime in the form of fraud. Fraudsters seek to monetize cybercrime and other crime by targeting our companies, our partners, and our customers. Annual fraud losses in the US represent a staggering $170B across all fraud types. Many of these fraud types apply to the provider's technical and financial operations including card fraud($32B), online fraud($26B), identity fraud($16B), check fraud($7B), synthetic fraud($6B), account takeover($5B), and new account fraud($3B)[1]. The methods to execute fraud vary from simple to very technical. In the fraud environment operators face today, fraud incidents are often proceeded by cybersecurity events. This requires a greater coordination and collaboration between fraud teams and cybersecurity teams. The fraudsters are creative and coordinated – they attack all aspects of our businesses, including care channels, video, wireless, Internet, mobile and voice services. This paper provides an overview of some examples of fraud experienced by cable operators, and then proposes a framework for fraud and a taxonomy, in order for it to be effectively described and discussed.

What is fraud? Why is it important? Operators are seeing an increase in external fraud resulting in service theft, device theft, and brand damage. In some cases, bad actors use compromised personal and payment information to create fraudulent accounts, or they may use Internet fraud resources to create fully synthetic identities. They may use modified devices to provide video and Internet services to customers they are servicing. Other approaches have been identified as well. In some cases, the subscribers working with the bad actor believe they are working with their actual carrier. Both wireline and wireless operators are being targeted across the globe.

There are many types of fraud being executed against cable operators and their partners. These may target the operators themselves, their customers, or even their business partners. We're focused on fraud that impacts the operator's service and the consumers of those services.

Different industry segments and their products experience fraud differently. Voice, internet, mobile, email, and video fraud all have characteristics that are unique to the operator and the product line. Supply chain and fulfillment may be part of fraud, as well – such as when a fraudster arranges for cell phones to be shipped to a certain location or sets up a new cable account resulting in shipment of cable modems and set top boxes.

2. Example Fraud Scenarios

This section examines three scenarios identified by service providers as being fairly common. Fraud follows the business context. It will be aligned and in context of the service or product being offered.

2.1. Fraud Example 1 – Account-Based Fraud

New accounts can be fraudulently created. These accounts are usually created to steal service. In these cases, the fraudsters often offer a product and service at a substantially reduced price. The fraudster will attempt to set up many fraudulent accounts to service their customers. These fraudulent accounts are set up with either stolen customer information or synthetic identities created for this purpose and to perform other fraudulent activities. In some cases, synthetic identities are set up and managed for years, for the sole purpose of defrauding companies over the lifetime of the synthetic identity.

2.2. Fraud Example 2 – Credential Based Fraud

A second common fraud leverages existing customer credentials. A common scenario starts with "credential stuffing" [2] and ends up as fraud against the customer or service provider. A customer's credentials are leaked from one of the "credential spills" that happen every month across the globe. These credentials are picked up by "credential testers," who will test the credentials against many websites, including those of the operator. If the credential is tested as valid on the operators' network, the "credential tester" will then post the credential for sale on a darknet marketplace. The credential is then bought by someone intent on committing fraud against the operator. The fraudster will use the credential to access the account and defraud the operator. This may be by ordering additional devices (mobile phones, set-tops, or cable modems). In the whitepaper "The Economy of Credential Stuffing Attacks" by the Insikt Group and available at Recorded Futures [3], the authors note that with an investment of $550 a "credential tester" can make up to $19,000 doing just the testing and sales of credentials in a matter of several weeks to months. A very lucrative investment indeed! This example helps illustrate the importance of collaboration between cybersecurity and fraud teams in deterring both the testing of credential as well as the fraud enabled by the validated credentials.

2.3. Fraud Example 3 – Brand-Enabled Fraud

Another example of fraud is one committed using the operator's brand to defraud the customer. An example of this is a fraudster who calls the operator's customer, poses as an operator representative and touts a special offer between the operator and a selected brand of gift cards. The fraudster will inform the customer that if they purchase gift cards and call back, they will reduce the customer's monthly bill substantially. Of course, there is no such offer. If the customer falls for the scam they will purchase the gift cards, call back a number they are provided, provide the information to the fraudster and the fraudster will claim that their bill will be lowered. When the actual bill from the operator arrives, there is no change. The customer calls the operator and then discovers the fraud, which frustrates the customer and damages the operator's brand.

3. The Business Context

There are many channels through which these frauds are conducted, which are depicted in Figure 1. Fraudsters may access the customer's operator web portal. They may call in and work with the interactive voice response (IVR) service or a customer care agent and escalate the call to full social engineering through direct, in-person interaction with retail employees, at kiosks or stores. On the other side, fraudsters may advertise services through social media, calling potential victims, or even doing door-to-door sales. Also, word of mouth by victims can lead to additional fraud: "Hey, I got this great deal on cable from this guy! Saved me lots of money. You should check them out. Here's the phone number."

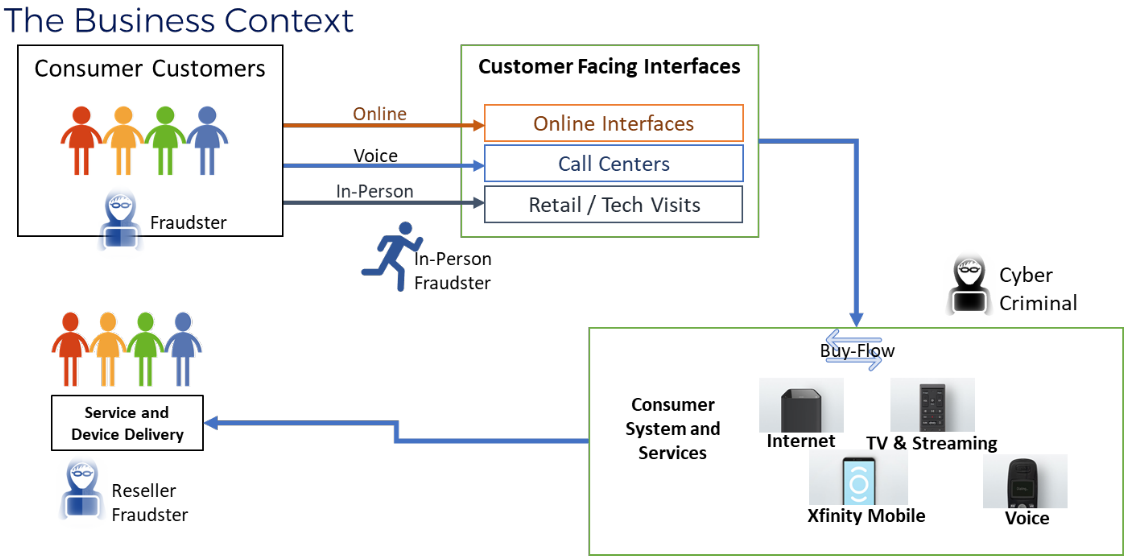


Figure 1 - Fraud in the Business Context

It's common to believe some of these frauds are victimless crimes. That is simply not the case. Service provider losses can be extensive and include theft of service, theft of equipment, loss of funds (through, for example, refund fraud), etc. Moreover, detecting, investigating, mitigating, and preventing fraud is quite expensive for operators. There are obvious victims, of course: victims of identity theft, stolen credit card information, cloned phones or cable modems, and more. One of the important aspects to keep in mind about frauds in this space is that they are usually done en masse. A given fraudster is likely to conduct hundreds or thousands of these frauds at a time, possibly against multiple service operators.

4. Fraud vs Cyber Security

There are many types of fraud, some very simple, some very complex. The Association of Certified Fraud Examiners (ACFE) defines fraud rather broadly: "In the broadest sense, fraud can encompass any crime for gain that uses deception as its principle modus operandus." Fraud involves, at some level, misrepresentation of fact in the course of conducting crime. This is an important distinction, in comparison to cybercrime. Cyber-attacks may, or may not, involve fraud. Fraud against an operator or its subscribers may or may not benefit from illegally obtained cyber or private information (though they often do).

One of the challenges that fraud and cyber teams face is the overlap between the work of the fraud professional and the work of the cyber security professional. In the hands of a technology savvy fraudster, the fraudster will often start their fraud attack as a cyber security attack. The cyber security attack, or a series of cyber security events, will end in a fraud event. For an operator whose products are primarily technology devices and services delivered via a technology base, the lines between what is a fraud event and a cyber security attack can be blurred. Given this context, there needs to be much greater collaboration between the cyber security teams and the fraud teams.

5. A Fraud Framework

An important distinction from the ACFE is that there are three primary types of fraud. *Internal fraud* is conducted typically by insiders and benefiting by the access those employees, partners, or contracts have to proprietary and unique resources. This is also known as *occupational fraud*. Another type is *external fraud* which is conducted by outsiders. Another large-scale distinction, *individual fraud,* is that fraud may be targeted against specific individuals. Operators can be impacted by individual fraud when their employees may be targets of individual fraud as part of attempts to defraud the operator. Fraudsters may also use an operator's services, reputation, or information illicitly to conduct individual fraud against subscribers. All three of these types of fraud are important to network operators.

In the business of a system operator, there are many products, and the technology platforms for service and device delivery are very complex. The "Fraud Framework" illustrated in Figure 2 provides a taxonomy for examining the customer contact points through which fraud will flow, as well as specific product areas, each with its own fraud challenges.

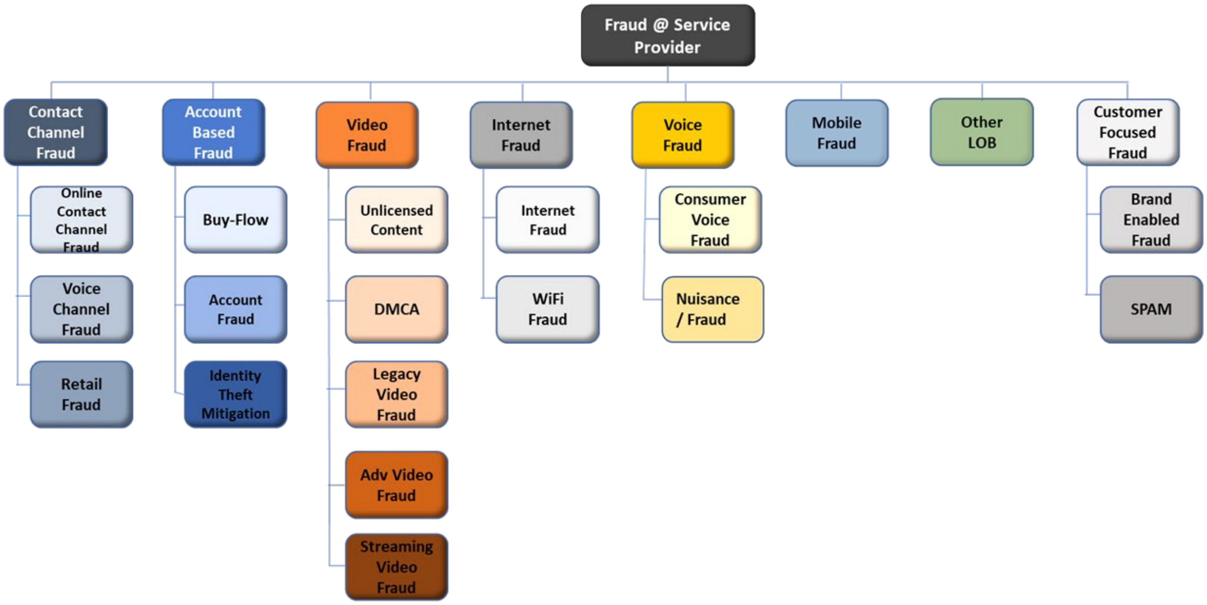


Figure 2 - A Fraud Framework

In collaboration between service providers, several fraud categories have been identified. Here is a list of only a few:

- **Contact Channel Fraud** – This is fraud that has as an entry point to the contact channels the service provider has created for its customers. The contact channel type will determine the class of fraud that is attempted through a contact channel. For the online contact channel, the attacks include credential stuffing, brute force attacks, and other cyber-based incidents. The voice contact channel will experience fraud attempts using social engineering as the primary tools. The retail contact channel will include social engineering, identity theft, synthetic identity, and cyber-attacks as the tools of fraud.
- **Account or Subscriber Fraud** - As described in the introduction, compromised private information, such as a Social Security number and payment form, are used to establish an account with a service provider. The payment method is fraudulent and is used to bypass the deposit

requirements. The fraudster resells the account with an end-user who pays for access. The fraud in this case is usually a representation, by the fraudster, of somebody else. Sometimes, there can be multiple frauds – the fraudster represents to the legitimate cable operator that they are a given party using stolen personal data, and represents to the end customer that they are an authorized agent or even employee of the cable operator.

- **Video Fraud –** Video fraud can manifest itself in many forms, including unlicensed content, notices from the Digital Millennium Copyright Act (DMCA) that the operator needs to process, legacy and advanced set-tops being used for illegitimate video service delivery, and finally streaming fraud enabled by credential sharing or credential fraud. There are many ways to monetize stolen content -- probably as many as there are to steal the content in the first place. The fraud here is that people distribute property and take payment for which they don't have the rights. Like voice fraud, there are several industry groups seeking to address video piracy and make the associated frauds simply unprofitable.
- **Internet Fraud –** Internet fraud includes the cloning or hacking of cable modems, as well as the illegitimate use of WiFi hotspots provided by the service provider.
- **Voice Fraud and Nuisance Voice -** There are many frauds conducted using fixed and mobile telephone networks. These range from toll fraud to spam to phishing and more. There are already several government agencies in many countries and group forums where operators, law enforcement, and regulators collaborate to address voice fraud. Voice fraud is obvious when someone calls a victim and misrepresents themselves. However, spoofing an originating phone number belonging to a known brand that is not owned by the fraudster to connect to a consumer is an effective way of committing fraud against unsuspecting consumers.
- **Mobile or Cell Phone Fraud -** This includes subscriber fraud, as described previously; it also includes cell phone cloning fraud. A common example today is SIM hijacking or SIM swapping, where a subscriber identity module (SIM) uses credentials from a legitimate subscriber's mobile phone's SIM card to activate one or more other cell phones. Because of the need for mobile service to support roaming, mobile networks have unique vulnerabilities to fraud that may impact multiple operators.
- **Customer-Focused Fraud** – in this class of fraud, the brand of the operator is used to gain confidence with the consumer either via voice contact or email. The confidence is used to defraud the consumer.

6. Details Relevant for Explaining Specific Frauds

Fraud is complicated. Many frauds are described by the Association of Certified Fraud Examiners and other groups. Two particularly good resources for understanding frauds are the Open Risk Manual [4] and the "Framework for a Taxonomy of Fraud" [5] developed by Stanford Center on Longevity, in collaboration with the Financial Industry Regulatory Authority (FINRA). Yet, cable operators experience frauds that are not even described by these resources. Our adversaries are very creative at finding ways to extract funds from our companies and our customers.

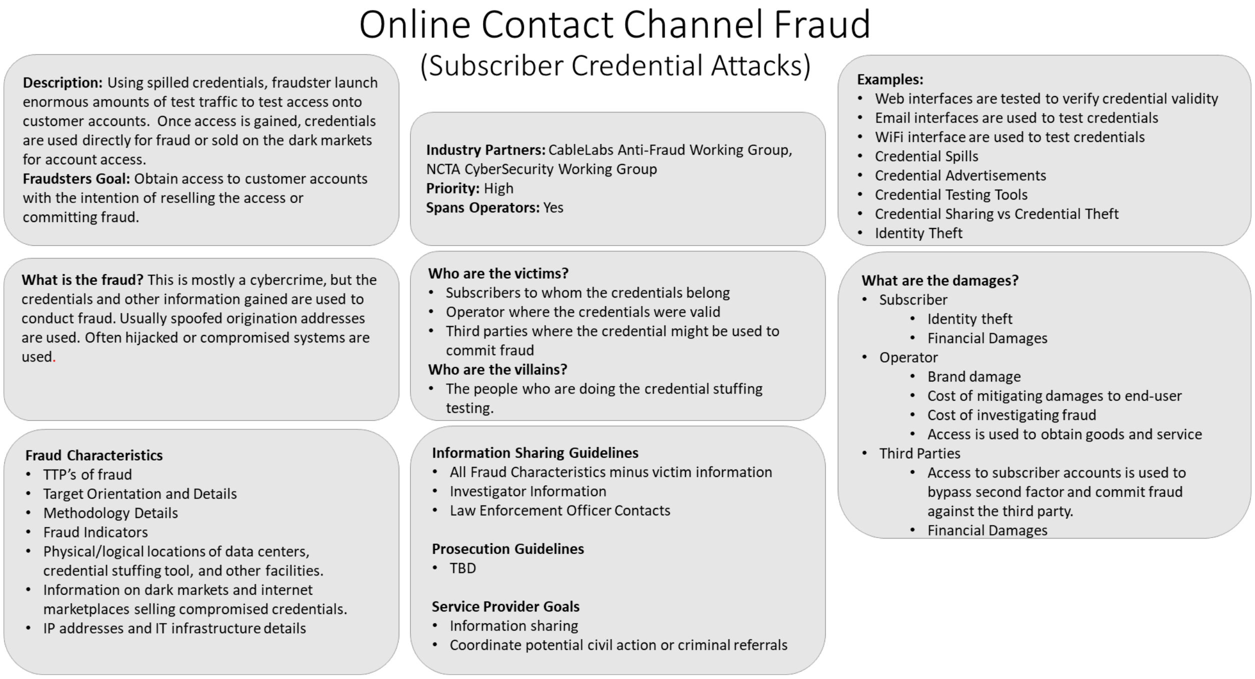
Can frauds be categorized and described in detail? What are the details that would be useful to cyber security and fraud professionals in describing types of fraud or related cybercrimes?

Like the frauds themselves, this gets complicated. However, an ontology and a taxonomy can be developed to describe and communicate about frauds. These details start with just basic descriptions and understanding the goal of the fraudsters. It's also useful at this level of detail to specifically identify the fraud that is being performed – exactly how is the criminal misleading their target, misrepresenting themselves, or otherwise specifically breaking the law. Who are the targets of the frauds and what type of fraudsters execute the fraud? (Yes, there are different skill sets and, as a consequence, different types of fraudsters.) It is useful to specify the damages to customers, the operator, or other parties (such as the government or vendors). Then there are details of the fraud methods themselves. These may include:

- Tactics, techniques, and procedures (TTPs) used to conduct fraud (TTP is also a cybersecurity term)
- Target Orientation and Details
- Methodology Details
- Fraud Indicators
- Physical/logical locations of data centers and other facilities
- Hacking tools used to execute the fraud (credential stuffing tools or markets, phishing frameworks, social engineering tools, etc.)
- Information on dark markets and Internet marketplaces selling compromised credentials or other enabling information for the fraud
- IP addresses and other IT infrastructure details

Then there are information elements useful to the examiners and investigators researching the fraud: Priority of the investigation, interested industry partners (perhaps other operators also being attacked), information sharing guidelines (what can or cannot be shared outside a company, for example). There are details related to enforcement actions such as prosecution guidelines, law enforcement or regulator contacts, and identities of investigators themselves. Finally, it is useful to understand the statistics and trends of the given fraud. This may include damages per event, cost to mitigate per event, estimated number of events annually, known cases, and the scale of the fraudster ecosystem perpetrating the fraud. Collected over time, these details can be used to identify trends.

This information can be collated and then presented in a very concise manner to quickly describe a type of fraud. For example, consider the description in Figure 3, below, of subscriber credential attacks as part of the "Online Contact Channel" category. In one page, specific information is presented that specifically conveys what a subscriber credential attack looks like. This is, of course, simply illustrative and lacks details of an actual fraud.



Online Contact Channel Fraud

(Subscriber Credential Attacks)

Description: Using spilled credentials, fraudster launch enormous amounts of test traffic to test access onto customer accounts. Once access is gained, credentials are used directly for fraud or sold on the dark markets for account access.
Fraudsters Goal: Obtain access to customer accounts with the intention of reselling the access or committing fraud.

Industry Partners: CableLabs Anti-Fraud Working Group, NCTA CyberSecurity Working Group
Priority: High
Spans Operators: Yes

Examples:

- Web interfaces are tested to verify credential validity
- Email interfaces are used to test credentials
- WiFi interface are used to test credentials
- Credential Spills
- Credential Advertisements
- Credential Testing Tools
- Credential Sharing vs Credential Theft
- Identity Theft

What is the fraud? This is mostly a cybercrime, but the credentials and other information gained are used to conduct fraud. Usually spoofed origination addresses are used. Often hijacked or compromised systems are used.

Who are the victims?

- Subscribers to whom the credentials belong
- Operator where the credentials were valid
- Third parties where the credential might be used to commit fraud

Who are the villains?

- The people who are doing the credential stuffing testing.

What are the damages?

- Subscriber
  - Identity theft
  - Financial Damages
- Operator
  - Brand damage
  - Cost of mitigating damages to end-user
  - Cost of investigating fraud
  - Access is used to obtain goods and service
- Third Parties
  - Access to subscriber accounts is used to bypass second factor and commit fraud against the third party.
  - Financial Damages

Fraud Characteristics

- TTP's of fraud
- Target Orientation and Details
- Methodology Details
- Fraud Indicators
- Physical/logical locations of data centers, credential stuffing tool, and other facilities.
- Information on dark markets and internet marketplaces selling compromised credentials.
- IP addresses and IT infrastructure details

Information Sharing Guidelines

- All Fraud Characteristics minus victim information
- Investigator Information
- Law Enforcement Officer Contacts

Prosecution Guidelines

- TBD

Service Provider Goals

- Information sharing
- Coordinate potential civil action or criminal referrals

Figure 3 - A Taxonomy Example of the Online Contact Channel Fraud

7. What Use is a Taxonomy?

A taxonomy, defined loosely here as a classification of fraudulent activities, can be very useful. It provides a way to specifically describe a fraud, which can be useful for deciding how to respond, and possibly even to support workflow automation. The "Framework for a Taxonomy of Fraud" [5] provides an excellent example of how this might be done by actually codifying fraud. Their system formalizes the ideas above and uses codes to classify the fraud and adds tags for describing the incident, victim, and perpetrator. An example they show in their report is "1.7.1. AD:IE. PS:M. MT:PC. FV. EF. MP." This string of characters is translated as:

1.7.1-> Classification Number

1->Individual Financial Fraud

7->Relationship & Trust Fraud

1-> Romance Scam

AD:IE -> Method of Advertising Fraud(AD): Internet, email(IE)

PS:M -> Purchase Setting(PS):Mail(M)

MT:PC -> Method of Money Transfer(MT): Personal Check(PC),

VT:FV, EF -> Victim Tags(VT):Female Victim(MV), Elder Victim 65+((EV)

PT:MP -> Perpetrator Tags(PT):Male Perp(MP)

While it may not always be beneficial to develop or use such a proforma format, the notion of specifically describing fraud is clearly useful for ensuring accurate communications between professionals investigating and prosecuting frauds. A taxonomy allows very clear discussion of exactly the nature and method of fraud. This can help operators solicit input from other operators to see if a given actor is conducting similar fraud in other markets, for example.

We've also found that a taxonomy can help to provide an organizational structure for how operators respond to fraud. Once they've codified what frauds they experience, they can organize accordingly. Moreover, the taxonomy can be useful for ensuring resource allocation and that workflows are optimized to deal with specific frauds.

8. Conclusion

Fraud is a challenge to all operators and will continue to be. It has a large impact to services providers who are at risk for both financial fraud and technology enabled fraud. A fraud taxonomy provides a way to classify a complex fraud system and improves the industry's ability to communicate, discuss, and improve the service provider's fraud detection and prevention capabilities. While an individual fraud attempt aimed at a service provider is targeted to that operator, the tools, techniques, and procedures(TTP) are common and shared between the fraudsters. The fraudsters share TTP's and so should we as an industry. The authors are seeking collaborators to take this work to greater levels of detail.

Abbreviations

ACFE	Association of Certified Fraud Examiners
DRM	Digital Rights Management
FINRA	Financial Industry Regulatory Authority
ID	Identification
IVR	Interactive Voice Response
LTE	Long Term Evolution
SIM	Subscriber Identification Module
TTP	Tactics, Techniques and Procedures

Bibliography & References

[1] "The Top 11 Fraud Types Here in the US and Their Losses", online: https://frankonfraud.com/fraud-trends/the-top-fraud-losses-for-2019-by-fraud-type/

[2] OWASP Credential Stuffing, online: https://owasp.org/www-community/attacks/Credential_stuffing

[3] "The Economy of Credential Stuffing Attacks", online: https://www.recordedfuture.com/credential-stuffing-attacks/

[4] Open Risk Manual, online: https://www.openriskmanual.org/wiki/Main_Page

[5] "Framework for a Taxonomy of Fraud", Stanford Center on Longevity and FINRA, 2015, online: http://longevity.stanford.edu/2015/07/30/framework-for-a-taxonomy-of-fraud/