Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2023, 10(7):57-61

Research Article ISSN: 2394 - 658X

# Biometrics for fighting financial frauds

**Goutham Sabbani**

Business analyst, Media Systems Integration, UK

**ABSTRACT**

If we look at the reported frauds for which contact methods were identified, a total of $13 billion has been lost due to frauds from 2017 to 2022. It is undeniable that frauds have been on the rise if we note that the total reports in 2022 were nearly 16 times that in 2001. 20 years ago, fraudsters relied on e-mails to establish contact and extract sensitive information. Now, phone calls and texts are the primary contact methods. However, fraudsters have always targeted information about account details, passwords, OTPs, and security questions. So, here we will explore how effective biometrics could be in enhancing security levels.

**Key words:** biometrics, frauds, fraud contact methods, fraud techniques

## INTRODUCTION

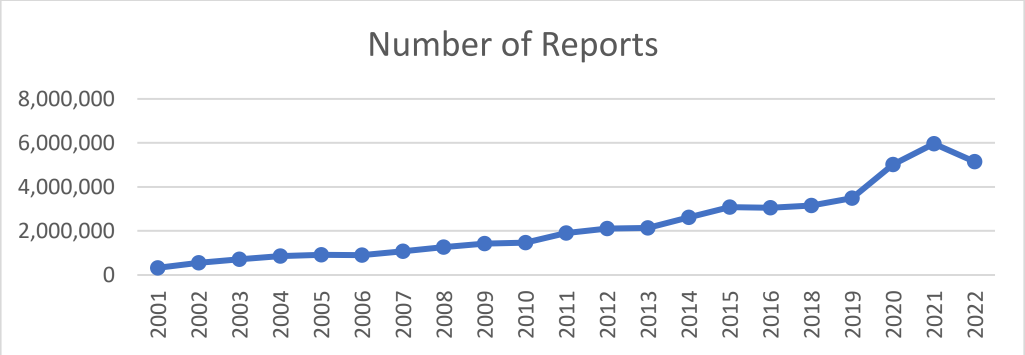
Over the last couple of decades, fraud reports have been on the rise. Experts such as Gadi Mazor note that legacy methods for ensuring the security of transactions cannot keep up with the speed and innovation of fraudsters. [4]

One of the measures being suggested to bolster the safety of transactions is biometrics. In this paper, we will review the trends in fraud over the last 20 years, note how fraudsters establish contact with victims, go over some common techniques they employ, and finally discuss the effectiveness of biometrics in increasing security. [1]

*Key fraud statistics*

The Federal Trade Commission (FTC), a US government agency, compiles reports from consumers regarding problems experienced in marketplaces. Let us observe some trends in the fraud statistics. As per FTC data, the number of reports increased nearly 16 times from 2001 to 2022, and more than doubled in the period between 2012 and 2022. [1]

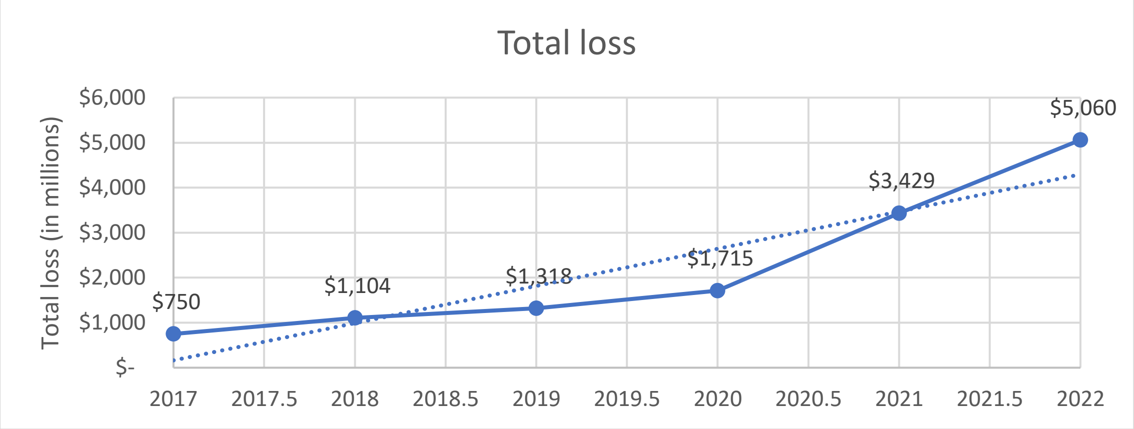
In 2022, five million reports were filed by consumers. In contrast, this number was less than half a million in 2001. In recent years, the biggest spike was recorded in 2020 when the reports increased by 44%, while the biggest ever spike in the recorded data was in 2002 when the reports increased by 69%.[1]



Source: Consumer Sentinel Network Reports (2008-2022) [1]

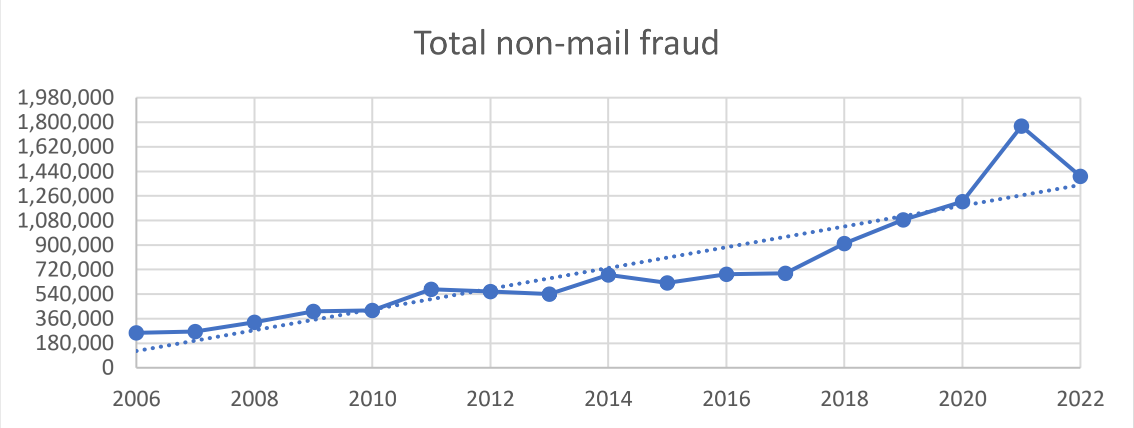
For this paper, we will focus on reports for which the contact method was identified. From the start of 2017 to the end of 2022, in the US alone, it was reported that approximately $13 billion were lost due to frauds perpetrated via phone calls, texts, mails, e-mails, social media, online ads, or pop-ups, websites, apps, and other mediums. [1]

The total loss from fraud has been climbing at an alarming pace. In 2017, the total loss from fraud was $750 million. By 2022, this figure had climbed beyond $5 billion. A significant portion of this rise in losses occurred between 2020 and 2022. [1]



Source: Consumer Sentinel Network Reports (2008-2022)

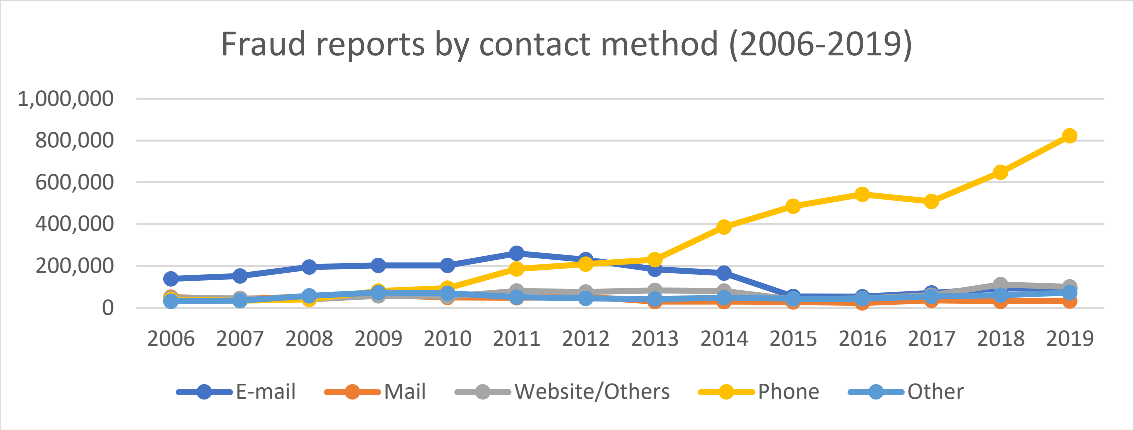
Since biometrics are best suited to defend against frauds perpetrated electronically, let us look at frauds where the contact method was not mail. From 2012 to 2022, the number of such frauds more than doubled. [1]



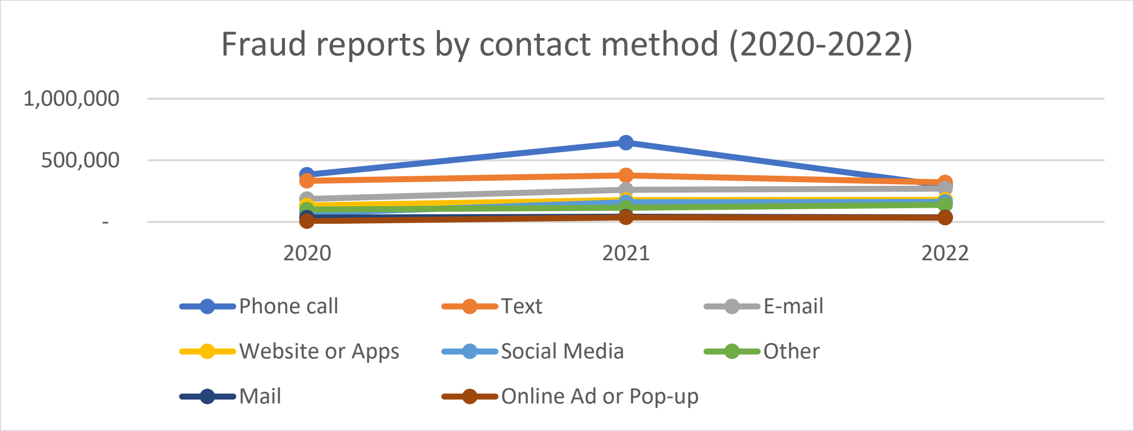
Source: Consumer Sentinel Network Reports (2008-2022) [1]

Back in 2006, e-mails were the preferred contact method for fraudsters. In 2006, e-mails were used for more than twice the number of frauds perpetrated via mails, the second most preferred contact method. However, since 2013, phones have overtaken e-mails as the preferred contact method. Mails, on the other hand, are the least-used major contact method of 2022. [1]

Data from 2020 allows us to dive deeper into contact methods. In 2020, phone calls were the most preferred contact method and in 2022, texts overtook phone calls. Other significant contact methods include e-mails, websites, apps, and social media. [1]



Source: Consumer Sentinel Network Reports (2008-2022) [1]



Source: Consumer Sentinel Network Reports (2008-2022) [1]

After analyzing the FTC's Consumer Sentinel Network Reports, we can establish two things. One is that frauds have been on the rise for the past two decades and this rise has only accelerated since 2020. Hence, advancements are an urgent need to make transactions safer. The second thing is that we can focus on the major contact methods of fraudsters when looking at popular fraud techniques to gain insights into weaknesses or areas targeted by fraudsters. [1]

## COMMON FRAUD TECHNIQUES BY CONTACT METHOD

Here we discuss some of the common fraud techniques used in different contact methods.

### 1. Phones

By swapping SIM cards, fraudsters can gain access to information like one-time passwords (OTPs) shared via SMS. This can be done by cloning a user's SIM card via software or by persuading the mobile network operator to send a new SIM card.

More sophisticated attacks would involve installing malware on phones to collect information using keystroke capture, and screen snapshots. Malware like this typically infiltrates a user's phone via off-market apps or downloads and transmits the data to fraudsters in the background.

Fraudsters could also clone the device itself, giving them access to data regarding all apps on the phone.

Man-in-the-middle (MitM) attacks capture communications between user phones and banks and financial institutions.

### 2. Website or apps

By analyzing and understanding the design and functions of a website and app, fraudsters could build a fake website or app. You might think that customers can tell a fake website from a real one by looking at the URL. However, this method is no longer reliable due to homoglyphs which are characters that look the same or similar but have different Unicode encoding.

For example, the Latin small letter 'a' and the Cyrillic small letter 'a' appear the same their Unicode encodings are U+0061 and U+0430, respectively. [2]

So, fraudsters could use the Cyrillic letter 'a' to create fake websites on Facebook, Amazon, eBay, or any other website that has 'a' in it. Mobile apps are even more difficult to tell apart since the URLs are not displayed in the first place.

### 3. Social media scams

Social media scams may involve manufacturing a fake persona, hacking into a user’s profile, and pretending to be a user to con others. FTC also notes that targeted advertising is being misused by scammers to effectively target victims based on their age, interests, and past purchases. [3]

According to FTC, in the first six months of 2023, approximately 56,000 scams were perpetrated via social media. Some common types of social media scams are online shopping scams, investment-related scams, and romance scams. [3]

Online shopping scams were the most common type of social media scams, making up 44% of the numbers. But investment-related scams which made up only 20% of the total number of scams reported, accounted for 53% of the total loss. The median loss in investment-related scams, romance scams, and online shopping scams were $3,000, $1,716, and $100. [3]

In October 2023, FTC found that one in four victims of frauds since 2021 reported that the fraud originated from social media and the total losses from social media frauds was $2.7 billion in the same period. [3]

### 4. E-mail

Fraudsters may approach victims by imitating banks and financial institutions. Their goal is to either install malware on the user’s device or con the user into sharing sensitive information like ATM PINs or OTPs. In some cases, such e-mails may have fake unsubscribe buttons that would lead to installing malware.

In some cases, fraudsters might try to lure victims through fake offers and promotions. Sometimes, fraudsters might impersonate government agencies and officials to invoke fear of fines. Here the goal is to trick the victim into sending money or worse, inputting their account details on the fraudster’s website.

Some e-mail frauds take the form of fake lotteries and persuade victims to share information like their name, address, phone number, gender, occupation, and bank account details.

Effectiveness of biometrics in fraud prevention

After looking at the common techniques employed in perpetrating fraud, we can see that the common targets are bank details, passwords, and OTPs. In some cases, fraudsters might also target information regarding security questions such as first pets, the mother’s maiden name, or the street name of the hospital where the victim was born.

By adding biometrics to the mix, we are adding another layer of defense. It should be noted that biometric information can be hard to fake or steal in comparison to data stored as text. For example, to capture a person’s fingerprint, a fraudster would need to employ a digital scanner or persuade the victim to share their ink-stained fingerprint. Fraudsters would carry a higher risk of trying to extract such data directly through bank databases. In either case, the fraudster runs a high risk of being made.

Other biometric data such as face, palm, and iris, too, are equally difficult to copy or fake. Institutions could go another step further by incorporating behavioral biometrics such as keystrokes or speech patterns. To bypass behavioral biometrics, fraudsters would be required to observe the behavior of their victims, and again risk raising suspicion.

However, it must be noted that while biometrics are difficult to fake or steal, they are not impenetrable.

According to Michael Weil, a managing director, and the Digital Forensics leader in the discovery practice of Deloitte Financial Advisory Services, “Leveraging biometrics for customer identity and access management (CIAM) is a good step. However, solely relying on biometrics and CIAM tools can lead to a false sense of security.” [4]

The final pieces or rather the next pieces in the puzzle would be consumer education, and higher levels of encryption of sensitive information. Supposing that biometrics held up to their expectations, end-users and institutions will still be targeted by fraudsters. Hence, the overall effectiveness of the security system would depend on how easily end-users can recognize fraud attempts and how secure the databases held by institutions are.

## CONCLUSION

The rising number of frauds requires innovation in security and safeguards. According to BioCatch CEO, Gadi Mazor, “The legacy technologies deployed within the banking community simply cannot match the innovation and speed of fraudsters.” [4]

In such a situation, biometrics can be a valuable additional line of defense. The value of biometrics comes from how hard they are to fake and the risk carried in extracting such information from end-users. But we must be careful not to bask in the false security and recognize that biometrics are just another tool in the toolbox, no matter how handy they turn out to be.

In addition to biometrics, institutions would need to continually invest in end-user education and database security measures.

## REFERENCES

[1]. Federal Trade Commission (FTC). "Consumer Sentinel Reports (2008-2022)." [Online]. Available: https://www.ftc.gov/enforcement/consumer-sentinel-network/reports

[2]. Unicode Consortium. "Unicode 15.1 Character Code Charts." [Online]. Available: https://www.unicode.org/charts/

[3]. Federal Trade Commission (FTC). "Social media: a golden goose for scammers." [Online]. Available: https://www.ftc.gov/news-events/data-visualizations/data-spotlight/2023/10/social-media-golden-goose-scammers

[4]. Global Association of Risk Professionals (GARP). "Behavioral Biometrics: A Safe Middle Ground for the Fight Against Financial Fraud?" [Online]. Available: https://www.garp.org/risk-intelligence/technology/behavioral-biometrics-fraud-092223