# New Account Fraud

One of the most prevalent frauds going on in the digital space now is new account fraud, also referred to as synthetic accounts. It can happen to anybody. All the fraudster requires is a little bit of your information — name, date of birth, and Social Security number — and with this they can fabricate a new account in your name.

## Vulnerability of Different Account Types:

No type of account is immune, credit cards, debit cards, loan applications, even a student loan application could be enough for a competent fraudster to get started on a synthetic identity. The competent fraudster will have numerous of these synthetic identities going at the same time. The confidence game builds the credit by actually paying bills. When the maximum available credit is obtained and all loans are in place, the fraudster will max out the credit cards, grab the cash and disappear. Given that the person never actually existed, there aren’t too many leads for investigative resources to follow up on.

If data is the new gold then we have to start talking about the consequences of mining this new gold. In the rush to cash in on data we don’t talk about the vulnerabilities of data as much as we should. In a world where more and more people are living online, without the biometrics that define them — appearance, voice, personality — data is all that is required to create a synthetic identity. It’s like the old criminal craft of forgery on steroids.

## Statistics and Financial Losses due to New Account Frauds

Statisticians place the number of synthetic accounts at 1.5 million or more cases per year since 2019, with losses on average more than 20 billion per year. As the fraudsters become more competent so too must the security. Adding to the problem is the seismic shift in online purchases that have happened since 2019.

There are a number of factors playing into this, not least of them was the pandemic and the stay-at-home orders, and then there is just the general confidence in online purchasing that has emerged in the last number of years. Like all things new the brave and the bold charge in first and the old guard waits until everything seems legitimate and then commences the practice as well — think cryptocurrency. Grandparents are buying online now, even if they didn’t get in early on Bitcoin.

## Security Responsibilities for Buyers and Sellers

Security is the responsibility of both the buyer and the seller. As the owner of a credit rating you should keep atop of all your credit scores. Maintain vigilance of billing. Make sure that you understand everything that is put in front of you and that you can account for all of the transactions. Never share personal information on social media sites and never pass personal information over a public Wi-Fi. Strong passwords are important, and if the vendor offers two step authentication use it.

## Fraud Detection Tools and Vulnerabilities

According to the *[2023 Global Ecommerce Payments And Fraud Report](https://merchantriskcouncil.org/learning/mrc-exclusive-reports/global-payments-and-fraud-report)* prepared by the Merchant Risk Council (MRC), Cybersource, and Verifi, merchants are using an array of [fraud detection tools](https://www.hcaptcha.com/enterprise), with over half using credit card and identity verification services. Enterprises go bigger. Smaller banks use fewer tools than most, and this places the smaller bank in a more vulnerable position. As technology emerges the larger financial institutions are the first to adopt — biometric indicators, individualized fraud scoring models, and multi merchant purchase velocity models — and smaller institutions may be forced to go out of business or find solutions to the increasing problems of security and the necessity of technology. This is the reality of the emerging data landscape replete with its inherent vulnerabilities.

The best in class technology for preventing accounts takeover are emerging out of the artificial intelligence (AI) and machine learning (ML) communities. [AI driven identity theft detection systems](https://www.hcaptcha.com/enterprise) operating at levels of pattern recognition heretofore unknown to digital security are able to detect anomalies early on, before the culprit penetrates the server or sensitive data. By allowing ML to study a bank customer’s transactions a pattern of behavior emerges. That pattern is far more complex than any human observation and data gathering could accomplish. This prevents credit card fraud before it happens or terminates the use of a credit instrument the moment an anomalous purchase is detected. The anomalies are not single source. They’re aggregated from a number of different sources, location, item, time of day and many more. ML is able to aggregate all of these patterns into a profile and it has unerring accuracy in defining when the user of a financial service is not the true profile.

## Future Outlook and the Role of Technology on New Account Fraud Mitigation

As the utility of data grows in our society so too will the vulnerability inherent in data. However, technology seems more than ready to tackle the security problems of digital commerce, open banking, and synthetic identity. It’s evolving so rapidly that it’s only a matter of time before models of investigation and arrest are formed all within the digital world. Just as the fraudster baits a financial institution into giving credit to a false account, we will soon be living in a world where digital intelligence through AI and ML will be setting these fraudsters up like undercover police stings.