TOOLCASE

How Real Time Analytics And Artificial Intelligence Solutions Can Prevent Sophisticated Child Tax Credit Fraud

by TOOLCASE

The objective of this report is to explain how real-time analytics and AI technologies can significantly reduce massive fraud loss connected to illegal activity aimed at collecting the IRS (Internal Revenue Service) Child Tax Credit.

This report also introduces a ToolCASE system that blends visualization and analytics with pattern, anomaly, profile, and behavior deviation recognition.

Fraud is not a new problem in the financial realm. However, with the increasing volume of digital transactions, cybercrime techniques are becoming more sophisticated with each passing minute—and fraudsters more knowledgeable about how to remain undetected.

Traditional anti-fraud methods, both those aimed at prevention and those aimed at detection, are falling short in the current digital ecosystem. Only a solid suite of Artificial Intelligence solutions that enables the aggregation of real-time transactional data with accuracy can curb the unparalleled costs of undetected future fraudulent activity.

THE IRS TAX CHILD CREDIT SCAM: A BILLION-DOLLAR PROBLEM.

According to the FTC (Federal Trade Commission), consumers lost US$3.3 billion to fraud in 2020, in sharp contrast to the US$ 1.8 billion lost in 2019. For taxpayers, banks, and credit unions, much of this fraud loss is tied to Child Tax Credit issues.

As part of the American Rescue Plan Act, from July 15th 2021 on, the IRS (Internal Revenue Service) has been disbursing Child Tax Credit payments. Depending on each tax-payer's specific situation, the amount of money paid by the IRS varies, ranging from US$3,000 to US$3,600 for parents with children under 5 years old.

To receive these payments, eligible taxpayers who have filed their 2020 tax report need not provide any new information or perform any further action; the money is automatically credited in their bank accounts following a monthly schedule that the IRS has made public.

US$3.3 billion

Fraud lost in 2020

However, those who have yet to file their 2019 or 2020 tax report, need to do so in order to be receive payments.

These taxpayers are especially vulnerable to fraudulent activity on the part of scammers, hackers, and thieves, who pose as IRS representatives offering help with benefiting from the credit rollout simply and fast.

Some fraud perpetrators go even further, changing taxpayers banking information on the IRS portal and funneling child tax credit payments into illicit accounts. Such activities add identity theft to the equation, creating an even bigger problem.

In fact, with identity theft as one of the preferred techniques used by fraud perpetrators, even childless taxpayers are at high risk of being a victim of child tax credit frauds.

Overlooking how advanced fraud criminals operate in digital contexts and avoiding acting with diligence can cause unprecedented financial damage.

The result is a billion-dollar loss problem.

The IRS itself has taken steps to educate taxpayers, banks, and credit unions on their website about the real possibility of fraud, especially warning against:

+ **Following email links**
+ **Providing sensitive information on social media channels**
+ **Answering text messages about advanced child tax credit payments**

While taxpayers have a certain degree of control over their online transactions, however, it is primarily the financial institution's duty to detect and prevent illegal or fraudulent activity.

According to the Datavisor Global Digital Fraud Trends Report 2021, each and every fraudulent account uses automation at some point in its life cycle.

Unfortunately for consumers, most companies have not modernized and strengthened their security measures, relying on obsolete technologies and practices to detect fraud even as the criminals themselves make use of the latest and most sophisticated automation tools.

As a result of outdated technology, an average of only 25% of fraudulent operations are prevented.

Until fraud prevention and detection methods begin to master the same technologies used by the perpetrators of fraud crimes, financial fraud problems will not only persist but will intensify.

FRAUD COMPLAINTS ARE ON THE RISE

2.2 million

reports of fraud were received by the FTC in 2020.

With this figure indicating a 46% increase in fraud reports from 2019 to 2020, it is patent that digital fraud is on the rise.

At the same time, according to the Consumer Sentinel Network (FTC), identity theft - the most frequently committed cybercrime - is dangerously on the rise.

In fact, the annual increase in users who officially reported that their personal information had been stolen and used to apply for government benefits in 2020 was 2,920%.

+46%

Fraud Complaints Reported in 2020

+2,920%

Identity Theft Complaints Reported in 2020

Source: Insurance Information Institute

With the Treasury and IRS announcing that almost 60 million families will be receiving a total of US$15 billion in credit, a massive volume of digital transactions are at risk.

These numbers reinforce the urgent need for effective prevention, detection, and prediction when it comes to fraud methods – especially where the new Tax Credit rollout is concerned.

TRADITIONAL FRAUD PREVENTION AND DETECTION METHODS

When dealing with the problem of fraud, there are two security layers to be considered:

1. **FPS (Fraud Prevention Systems)**
2. **FDS (Fraud Detection Systems)**

The first security layer of security is **FPSs (Fraud Prevention Systems),** including the traditional use of firewalls and/or encryption and decryption processes. These methods are the most commonly used, but not the most effective.

- **Firewalls:** Firewalls can be hardware or software especially set up to filter out unwanted intruders, like scammers and thieves. They make unauthorized access difficult but not impossible.
- **Encryption & Decryption:** Encryption involves the encoding messages so that only authorized users are able to see them. Decryption is the inverse process, in which messages are decoded for use by authorized users. As with firewalls, they cannot fully prevent unauthorized access, but they can minimize it.

The second security layer is **FDSs (Fraud Detection Systems)**, including anomaly detection and misuse detection. These are more sophisticated anti-fraud processes than those in the first layer, and it is here that Machine Learning enters the picture of fraud detection. These approaches radically increase the effectiveness of anti-fraud activities.

- **Anomaly detection:** Also called outlier analysis, anomaly detection can identify data points, observations, or events that do not follow a dataset's expected behavior.

  When implemented well, this data-mining process can detect critical incidents and identify potential glitches by classifying behavior as normal or suspicious.

  Anomaly detection can be supervised, unsupervised, or semi supervised.

- **Misuse detection:** This approach, also called signature detection, learns patterns about past suspicious data behaviors and these acquired patterns are used to predict and/or detect similar behavior in the future that could be a fraudulent activity indicator.

THE PROBLEM WITH TRADITIONAL METHODS IN THE DIGITAL ERA

The first layer of FPS is very easy to break by fraudsters. The second layer of FDS, while much more effective, requires a time-consuming implementation that sometimes cannot keep up with the rhythm and massive volume of digital transactions.

Traditional methods are failing short because they lack what our fast-paced digital era demands: accurate predictive models.

Crucially, accurate predictive models and the real-time detection of fraudulent activity are only possible through the effective implementation of AI and ML tools.

AI and ML can prevent current child tax credit fraudulent techniques both before and while they are happening using behavior analytics. They quickly identify the normal patterns of genuine transactions, and when suspicious activity is detected, fraudsters are uncovered before having the opportunity to commit any crime.

The Solution: RembrandtAI

Artificial Intelligence is here to stay. Whether taking full ownership of mitigation decisions or using a human facilitator to accelerate the decision-making process based on gathered data, AI offers significant benefits compared to traditional fraud prevention methods.

RembrandtAI is no exception.

The anatomy of the revolutionary RembrandtAI technology is based on three major sophisticated pillars:

Speed: Speed makes it possible to analyze millions of transactions, across all data channels, in real-time. It enables appropriate and diligent action when anomalous activities arise, are attempted, or are anticipated.

Machine Learning Abilities: Artificial neural networks make a fast comparison between all transactions, whether legitimate or fraudulent. Once patterns are established, any transaction can be analyzed to see if it fits the pattern of a legitimate transaction or if it might be fraudulent, enabling financial institutions to stay ahead of cyber criminals.

Model Evolution: Model management involves several phases of development, training, versioning, and deployment of Machine Learning models. Because of this intense modelling process, accurate predictions can be made and possible fraudulent activity can be detected before it occurs.

Through these pillars, RembrandtAI technology can assist individuals and organizations guard against the painful consequences of child tax credit scams by detecting suspicious activity, such as modifications to financial details, and thus strengthening verification steps for information generated through government portals, bank account details, and other sensitive data.

INTRODUCING RembrandtX

RembrandtX is a new data aggregation solution with unparalleled capabilities in seamless data accumulation and integration from multiple distributed sources of both static and streaming data.

The RembrandtX Advantage

A key advantage of the RembrandtX solution is that it can integrate data from:

- + Databases
- + Sensors
- + Scheduled job runs
- + Batch-oriented mainframes
- + File storage
- + Manual uploads

What is the advantage? With RembrandtX's sophisticated data aggregation capabilities, static and streaming data can be matched in real-time with market data and public resources to enable dynamic analytics in tandem with the RembrandtAI solution suite.

When it comes to Child Tax Credit scams, as well as detecting any suspicious activity, AI solutions like RembrandtX can identify the pattern of different fraudulent scenarios in a way traditional approaches will never do, uncovering hidden correlations and analyzing user behavior that not only separates normal from criminal transactions but also improves data credibility.

Detecting fraud in real time is the reason why financial institutions have trusted ToolCASE solutions to safeguard their clients for twenty years.

Having processed over 60 billion transactions, ToolCase has helped to avoid more than **US$150,000,000** in losses for the retail banking industry.

At ToolCASE, we're on a mission to change the world by defining the next era of diversity, leveraging data, analytics, and cognitive technology for greater innovation.

Contact us to request:

+ a free demo
+ pricing information
+ technical support

CONTACT US