WWW.TOOLCASE.COM

Less Fraud, Less Friction

Analysis of Card Fraud

Whitepaper by TOOL**CASE**

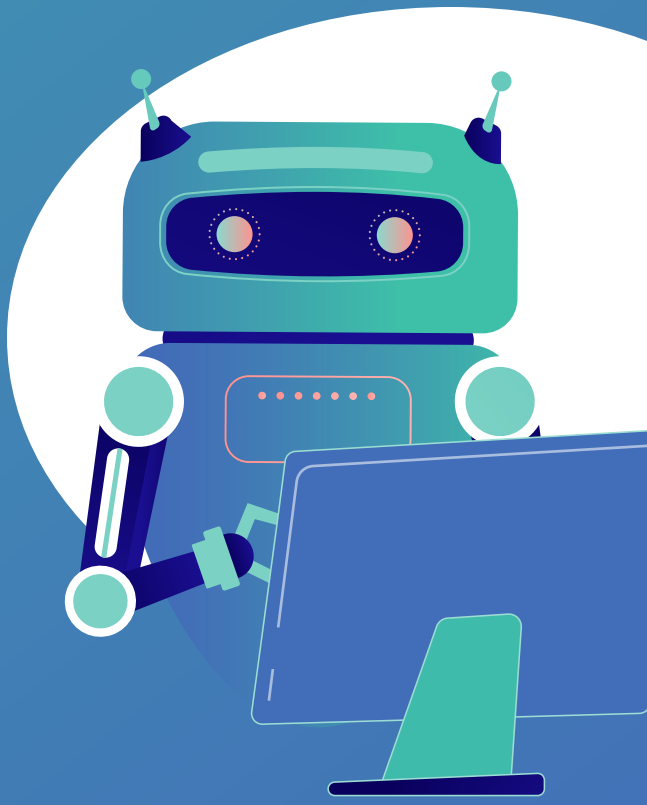
TOOLCASE

Recent times have brought about a higher demand for online payment options. However, much to the dismay of consumers, credit card fraud and payment friction remain at an all-time high.

These undesirable developments have given rise to a demand for more cybersecurity and real-time credit card fraud prevention technologies.

Addressing fraud has long been in the minds of business owners and institutions. However, lasting solutions to it have yet to emerge — until now. Tools that leverage the power of AI can now hit two birds with one stone as they both prevent fraud and reduce payment friction.

Never has the use of AI in fraud prevention been more important than now.



Identity Theft: A Problem That Is Bigger Than Ever

The COVID-19 pandemic has given rise to increased consumer spending on online channels. For this reason, companies have been quick to bulk up the e-commerce integrations of their sites, setting pathways for online payments.

Online payment methods have diversified – particularly in 2020 – branching beyond traditional credit card payments to include debit cards and now digital wallets.

Unfortunately, the number of fraud incidences — identity theft, specifically — are concurrent to the surge in online transactions. In 2020, 68% of all transactional fraud were incidences of identity theft, equaling at least 1.3 million reported cases. The percentage represented a surge of at least 60% within a year alone.

What's concerning is the fact that many cases of identity theft are unreported. The current statistics may just be the tip of the iceberg.

As well, credit card fraud has rendered young adults aged 30 to 39 susceptible to identity theft. According to recent statistics, senior citizens were also not immune from the threat of losing their benefits programs through identity theft.

Those under the age of 19 were also victims of identity theft, with no less than 23,000 cases tallied in 2020. Equally concerning to individuals and institutions is the number of stolen child data. In 2020, it was reported that 1.3 million children had their information used fraudulently.

Identity thieves target many accounts. Of note are five that are pivotal to individuals and institutions, namely social security benefits, employment records, credit cards, bank details, and tax-related accounts. The vast majority of identity theft reports involve at least one of these accounts or personal information.

The problem of identity theft continues to loom, with cases being ubiquitous across the board. In fact, according to a 2020 survey, seven in 10 Americans report falling prey to identity theft at some point in their lifetime.

These statistics paint a bleak picture of data security. Identity theft continues to plague more people. This problem is predicted to grow in the years to come and does not show signs of stopping.

Consumers can become victims of identity theft for a myriad of reasons, a major one being credit card transactions that are intercepted and exploited by hackers.

In the next section, the magnitude of credit card fraud will be discussed in greater detail.

Credit Card Fraud Accounts for Nearly a Third of Identity Theft Reports

In 2020, credit card fraud reports skyrocketed to at least 400,000 incidences. This represents an increase of as much as 32.5% from its original record of 270,000 in 2019. With credit card fraud making up nearly a third of all identity theft incidents, it dominates other causes of identity theft. Worse yet, the United States leads other countries in credit card fraud reports and losses as losses have totaled more than an estimated $11 billion in 2020.

400,000

incidences

32.5%

increase

$11 Billion

total losses

Credit card fraud is prevalent in several states. In particular, Delaware, Florida, Georgia, Nevada, and Maryland all recorded the highest figures per capita for credit card fraud.

Senior citizens were particularly vulnerable to credit card fraud. According to the most recent statistics, not only was this group more prone to being victims of fraudulent transactions; senior citizens were also the most susceptible to financial losses resulting from fraud.

New account owners and regular users were not spared either. According to recent statistics, New accounts were more at risk for fraudulent credit card transactions, with incidences spiking by as much as 48% from 2019. Sources attribute this uptick in fraud incidences to increased digital transactions and wider adoption of online credit card payments, where physical cards are not present.

Fraud does not stop with online credit card transactions. It also made its way to COVID-19 benefits and stimulus payments. In 2020, there were an estimated 144,000 reports of fraud affecting stimulus payments.

In short, it would seem that the mere possession of a credit card automatically makes one susceptible to credit card fraud and identity theft. Given the indispensability of credit cards and other items for transactions, real-time fraud protection is a necessity. It is an even bigger necessity now due to the prevalence of card not present (CNP) transactions.

The Vulnerability of CNP Transactions

Of any card-related online transaction, CNP transactions were the most vulnerable to fraud in 2020. As the leading type of credit card fraud in the United States, CNP fraud has led to losses of up to $10 billion annualy.

The ease with which fraudsters can use CNP transactions for profit can be traced back to the absence of the physical card. At the moment of purchase, the buyer does not present the actual card. In place of the card, the buyer presents details linked to the card like its number, associated name and address and CCV.

As a result, a devious online merchant or criminal can obtain payment, without signature or photo verification. Unfortunately, when the merchant/fraudster plans to commit fraud, the legitimate cardholder is left with little to no protection. This is because cards will often come with safety features that provide a layer of security to a physical transaction, but not for CNP transactions.

Such features include identifying markers like the EMV chip — a chip that is unique to every card. Without the chip and some form of authorization from the card's user, no transaction takes place.

In a CNP transaction, the provision of card-related details allows a fraudulent merchant to bypass the security features of a credit or debit card. As a result, when a transaction is shown to be fraudulent, the buyer or the card's user has no other option to turn to but a chargeback. A chargeback refers to the return of money following a transaction that has been proven fraudulent, and can hurt both legitimate merchants and card companies.

Unfortunately, proving fraud in a CNP transaction has obstacles owing to the absence of the physical card. This can reduce faith in the CNP system — and it has done so in 2020.

Hence, the losses resulting from credit card fraud result in losses beyond consumer money.

Losses Beyond Money

Credit card fraud and identity theft have led to massive financial losses. As of 2020, money lost in fraudulent transactions has amounted to as much as $11 billion. Such financial losses have created undesirable changes, particularly in the areas of frictionless payments.

With the public now aware of fraud's prevalence, the trust in online payments has dipped. As consumer confidence drops, e-payment options become less attractive to shoppers and merchants.

The loss of trust in card transactions can also affect businesses whose main platform for doing business is online. Since the risk of fraud remains high, consumers will be hesitant to patronize a business that cannot guarantee security, which is perhaps every online-based merchant.

In short, losses occur on three fronts. On the part of the consumer, there is additional payment friction owing to hesitation and awareness of risks. For the merchant, low consumer confidence in online payments means less chances to collect online payments. And for card issuers, there's both a loss of confidence by cardholders and the threat of holding the bag.

Companies and User Data

Data breaches are higher now than they have ever been. Although breaches have dipped by 5% globally, the United States has recorded a sharp rise in data breaches, with government agencies and financial institutions being prime targets.

With more companies obtaining user data, hackers have large companies in their sights. Hackers can now intercept transactions and use information like credit card details for their profit. Data breaches have been recorded and involve some of the biggest companies today.

Usually, stolen data has little effect on the average user. However, for those affected, the losses and damages can be catastrophic. Everything from personal information to card details is open for hackers to exploit. Equally concerning is the rate of increase in data breaches within one year.

Between 2020 and 2021, there have been 1,862 reports of data breaches. This represents a sharp uptick of as many as 500 incidences. This statistic even trumps the 2017 high of 1,506 incidences.

Indeed, these figures are small by global standards. However, it is important to note that these are simply reported cases. According to the Identity Theft Resource Center's 2020 and 2021 statistics, most cases of breaches go unreported.

In addition, an equally important note is the fact that the number of cases does not involve individuals. Instead, these are institutions. In regard to the number of individuals affected by data breaches, the most recent statistics have the numbers at 155.8 million.

Between a Rock and a Hard Place: The Online Payment Dilemma

As mentioned earlier, the rising cases of credit card fraud and identity theft threaten consumers' confidence in online payments. While it is reasonable to think that the way out, for consumers at least, is through cash payments. However, its not that simple.

The COVID-19 pandemic has decreased the physical exchange of cash.

Since its declaration as a pandemic in 2020, COVID-19 has made more people conscious of their physical contact with people and objects. This hyper-awareness has caused physical cash exchanges to decrease at a rate unheard of in history.

For example, in the United Kingdom alone, cash flow decreased by as much as 60% in 2020. This meant that businesses were only able to collect payments digitally. The trend was no different in the United States as nearly a third of the population stopped using cash.

These trends have resulted in a greater reliance digital and on online payments. In the United Kingdom, online payments in stores shot up to 28% — 9% more than it was the year prior.

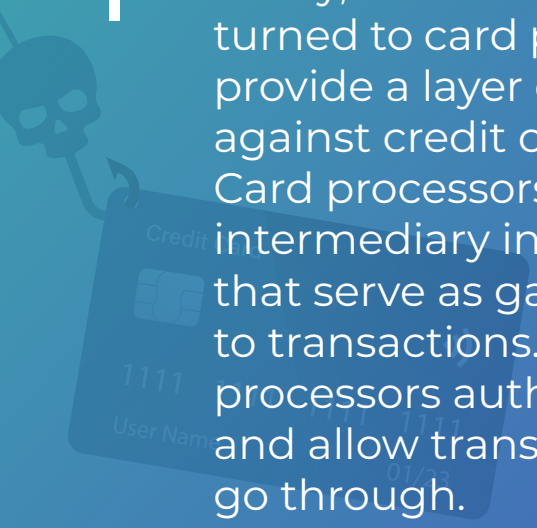
The shift towards online payments occurred all over the world. With a greater dependence on online payments, there came a paradigm shift in how people accessed and used money. This resulted in a massive shift towards digital banking.

The mass adoption of digital banking and digital transactions occurred due to COVID. Nevertheless, the gradual return to normalcy did very little to bring people back to cash. Owing to habit and convenience, people remained reliant on digital payment methods like credit cards, debit cards and e-wallets.

In short, as digital payments become the norm, consumers are met with a dilemma. On one hand, the risks of credit card fraud and identity theft are real. On the other, paying digitally remains a convenient necessity.

With only digital payments as options for many, credit card fraud prevention strategies are crucial in today's market.

The Problem With Card Processing as a Solution



Lately, businesses have turned to card processors to provide a layer of protection against credit card fraud. Card processors act as intermediary institutions that serve as gateways to transactions. Card processors authenticate and allow transactions to go through.

Whether or not transactions are completed depends on the presence of ID markers. For physical credit card transactions, one such marker is the EMV chip. For CNP transactions, it may be details like the card number or the CVV/CVC code.

While the intermediary model under which card processors operate works on paper, it is not a complete solution to fraud. Based on rising fraud claims, the solution only seems to work for the few people who are made aware of fraudulent activities with their accounts.

In 2020 alone, 127 million people reported at least one fraudulent charge involving their credit or debit cards. Of this number, 41 million reported that they were the victims of more than one fraud transaction.

The minority who have managed to avoid fraud were those who had their fraud notifications enabled. However, even for this group, identity theft and credit card fraud were only averted after the card users took action to inform their banks, causing friction between the consumer and financial institution.

Even with notifications and alerting card issuers or banks, preventing fraud is not a guarantee. According to recent statistics, only 55% of fraud charges were blocked by card processors, with the remaining 45% remaining unresolved.

In short, card processing is, at best, a deterrent to fraudulent activity. It does little to prevent it. Once charges have been made to users' cards, card users need to alert their banks or card issuers, adding inconvenience to recovering losses.

The Necessary Paradigm Shifts in Credit Card Fraud Prevention

As credit card fraud remains at large, businesses are in a mad scramble to restore the trust of their customers. By reducing payment friction and guaranteeing safe transactions, businesses can achieve this. An effective fraud prevention strategy begins with two things — mindset and an added emphasis on detection.

Prioritizing Credit Card Fraud Prevention

Businesses easily fall into the trap of allocating towards "cash-yielding" processes. In other words, companies prioritize spending based on what will bring in the most revenue.

This way of thinking puts fraud prevention on the back burner. Also, it is this mindset that makes the digital payment streams and account data of these companies vulnerable in the first place. For this reason, companies need to invest more in technologies that put fraud prevention on the front-burner, while still allowing for "cash-yielding" transactions.

By shifting priorities towards fraud prevention, companies can retain customers, profits, and their corporate image.

Investment and Emphasis in Detection

With data breaches and credit card fraud on the rise, companies will be shooting themselves in the foot by being reactive.

Acting on breaches or incidences of fraud only when incidents arise will do little to ease friction. This is why companies need to shift their investments towards resources — human and technological — capable of analyzing and detecting threats.

Our Credit Card Fraud Prevention Strategy — Data Aggregation

A more total-solution approach to credit card fraud prevention must leverage two technologies. The first being data aggregation. Data aggregation allows data from all institutions involved in a transaction to be consolidated in one place. This makes fraud detection quick, efficient, and less costly.

Application programming interfaces (APIs) link the different parties involved in a transaction. The data created by APIs facilitate the data aggregation process.

Upon a single transaction, API data is obtained from the card owner, banks, and the card processor. The transaction data collected forms one data point which can be efficiently analyzed.

The resulting data point is change-sensitive, meaning that any attempt to intercept a transaction will alert our system instantly. As a result, hackers will have little to no margin to steal and use credit card data.

AI Fraud Prevention Fueled With Real-time Data Analytics

Data aggregation is only part of our credit card prevention solution. Our fraud prevention systems also feature AI-powered analytics fueled by the latest machine learning integrations.

With AI, credit card fraud shows up on the radar live. Detection happens faster than hackers can complete a data breach. With immediate detection comes immediate intervention.

The speed at which our AI integrations detect discrepancies in API-generated transaction data trumps that of batch systems. On top of real-time detection, our multi-level AI systems — like RembrandtAi — maintain a record of findings via its write-back feature. With this feature, the details of a breach are stored and incorporated into a detection algorithm for future use.

With ever evolving algorithms at our disposal, our AI renders future threats more predictable, ensuring even faster credit card fraud detection and prevention.

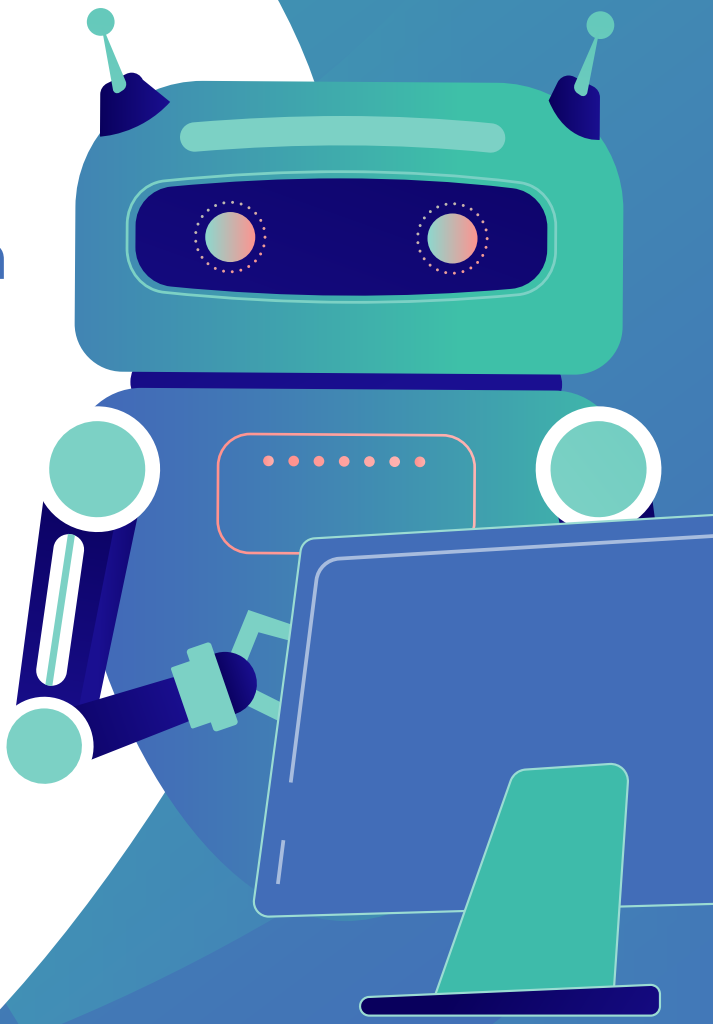
In short, our AI fraud prevention systems do the following:

- Detect and prevent threats
- Discover discrepancies in API-generated data (i.e. data agglomeration)
- Add findings to a data cache for later use
- Use the data for detecting and preventing future threats

All in all, our AI systems provide a multi-layer solution to credit card fraud prevention and detection. Hence, our systems, RembrandtAI and RembrandtX, are valuable for companies looking to stop credit card fraud, data breaches, and identity theft dead in their tracks.

Most importantly, they can reduce the friction between card holders, merchants and issuers.

The Future Is Multi-layer Fraud Prevention Powered by Data Aggregation and AI



Our solutions are a quantum leap in fraud detection and prevention. In today's world, taking a piecemeal approach to credit card fraud prevention does not suffice. With data emerging from numerous points, a multi-layer AI-based solution is perhaps the only way toward better consumer protection, continued online commerce and a preserved corporate image.

CONTACT US

TOOLCASE