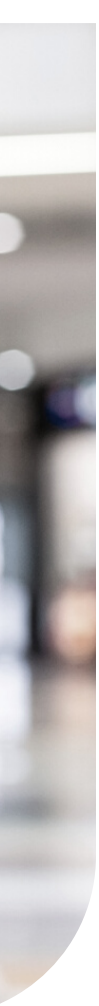
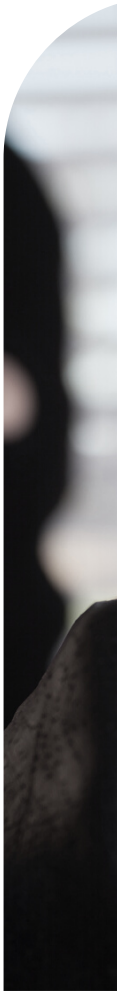
The Elimination of In-Store Credit Application Fraud

Real World Case Study

How a consumer electronics retailer utilized Identity Authentication to stop in-store credit fraud perpetrated with fake ID Documents





FRAUD FIGHTER™

Sean Trundy, C.O.O.
FraudFighter Products
2022

CONTENTS

About the Author

Sean Trundy is a 20-year veteran of the forged document fraud prevention industry, and is C.O.O. of FraudFighter Products, the leader in counterfeit detection. Mr. Trundy has been directly involved in consulting and designing fraud prevention solutions at over 500 different organizations, including Fortune 100 giants such as Macys, T-Mobile, Hertz, Wells Fargo, Avis Budget, Citizens, Regions, Chase and more.

Executive Summary

Facing steadily increasing chargebacks as the result of fraudulent in-store credit applications, RetailCo, a chain of retail consumer electronics stores, sought a solution that would halt incidences of account application fraud without impacting the otherwise successful in-store customer credit program. The fraud problem was serious.

According to the Director of Loss Prevention and Risk Strategy for RetailCo, prior to implementing the PALIDIN solution into their store locations, occurrences of fraudulent loan applications averaged 12-15 cases per month.

CUSTOMER CONFIDENTIALITY

In order to maintain the anonymity and confidentiality of our client, specific information regarding the name and the operational details of this customer has been redacted. However, should you be interested in learning more, the Director of Loss Prevention has made himself available to discuss his experiences. Please contact John Herlihy, V.P. Major Accounts for FraudFighter, at johnh@uveritech.com, if you wish to speak with this well-respected Loss Prevention professional.

As the Director of LP saw it, the heart of the problem lay in the inability of store employees to verify the authenticity of in-store credit applicants' identities. Because of this, the process of accepting new credit applications was vulnerable to the new breed of organized identity theft that has become endemic in North America.

RetailCo decided to conduct a pilot project in 12 of their locations utilizing the PALIDIN Desktop's ID image capture and authentication product. The ID-150 scanner captures high-resolution pictures of a customer's ID document, then PALIDIN conducts a forensic-level authentication of the document by comparing the images to a database which includes known physical characteristics and security features for U.S., North American and International ID documents.

The results of the pilot project were both immediate, and impressive. Fraud in the 12 stores was halted completely.

Based on these successful results, RetailCo approached their credit underwriting bank-partner. They made the case that preventing the credit fraud in their stores benefited the bank as much as it benefited RetailCo, and pressed the bank for the funds to purchase enough of the PALIDIN Desktop licenses and ID-150 scanners necessary to protect the remaining stores. The bank agreed, and the equipment was purchased.

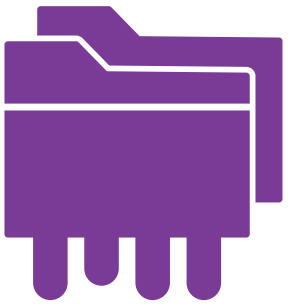
4 months after the completed roll-out to all locations, RetailCo has reported that incidences of credit application fraud have been reduced by 54%. Break-even on the project was realized in less than 2 months, and the 4th month after implementation – by which time all stores were operating effectively **- the reduction was greater than 90%**

Modern Identity Theft

In recent years, there has been a tremendous proliferation in the volume and quality of stolen identity data, making it possible for professional identity theft rings to exploit vulnerabilities in the financial services marketplace.

Due to the detail of the identity data that has been stolen from organizations, both in the U.S. and internationally, it is possible for organized criminal rings to assemble “identity fulls” - complete files on an individual - which contain not only key data, such as social security number, date of birth and home address, but which may also include such things as pin numbers and passwords, answers to secret questions, and compilations of public-records data. All of this information helps identity thieves get past most of the methods used by financial service organizations to identify false identities.

During 2022 in America, hackers were able to infiltrate supposedly secure networks at retail companies, merchant processors, and financial service providers and compromise greater than 422 million records containing private identity information. As many as one out of every three American adults may have had personal identifying information stolen. The implications are astonishing. Due to the unprecedented affect these breaches may have on the lives of many Americans, this is one of the most disturbing economic events to have occurred in years.



Expect a Spike in Activity

According to a recently released report by Dell SecureWorks, one immediate effect of this glut of identity data is already being felt. The price of a complete identity profile containing name, home address, email addresses, phone numbers, date of birth, Social Security number, and information on bank and credit card accounts has dropped by almost 40%, to the unprecedented price of just $25.00.

With such a sharp drop in the cost of stolen identities, it would be reasonable to expect an increase in the number of identity fraud attempts, not only for traditional opportunities (such as home equity loans, credit card applications and vehicle purchases), but also in circumstances that may previously have been considered too small or not lucrative enough to justify the work and expense of acquiring the identity (such as “buy online, pickup in store”, cellular phone contracts, and utility service accounts).

Big-Data Meets Organized Crime

The criminal community has embraced digital technology at rates so alarming it has caught most organizations unprepared. This has been evidenced by the data breaches which have made front page news in recent months. However, where the adoption of digital technology has really taken off is seen in what happens to the data after it has been stolen.

As recently as just 7 or 8 years ago, much of the data would have gone unused, due simply to the fact that the hacker often did not have the distribution network necessary to disseminate tens of thousands of identities to the "cashers" who actually use the data to convert it into fraudulent gains.

Add social media and eCommerce to the picture. Now, numerous "Dark Markets" exist to provide this very service to the data thieves. Imagine that you have just hacked 10 million records from a large retailer. The dark markets serve as a place where the data can be collated, stored and sold. Data is purchased by the dark market operator, who then treats the data the same way any other Big Data
management firm might – trying to match records hacked from multiple different sources in order to build complete ID profiles – called *"fullz"* in the market parlance of the underground data thieves.

The (dark) Market for IDentity Data

Because many dark markets are operated by international organized crime rings, they have a ready-built network of potential "cashers", located around the globe, who are ready, able and willing to convert this bounty into monetary gains. Using common social media apps like Twitter or FaceBook, the word will go out that the market will be online soon. Interested parties make direct contact and receive log-in credentials. Typically, such dark markets are located on the deep web, that portion of the Internet which cannot be seen or indexed by search engines.

Typically, the dark market will only be hosted during specific operating hours, and will often utilize the DarkNet – an anonymous peer-to-peer hosting process that makes it difficult-to-impossible to discover where the initiating fileserver is located.

Once logged-in to the dark market, the potential buyer will see an interface very similar to eBay or Amazon. Vendors with data to sell may have banner ads, offer fee trials, or even make coupon codes available. Search engines within the market will allow the potential casher to locate victims in their geographic locale, which allows them to partially circumvent the forensic algorithms relied on by payment processors and financial institutions to detect fraud.

In one famous case, a dark market (now, busted, thankfully) hired data scrapers to go out and find public records data, such as place of birth, previous residence addresses, previous phone numbers, mortgage balances, etc. which would arm the "casher" with information required to answer questions posed by identity verification software utilized as part of the credit-application process in many financial institutions.

Enter the Professional Forger

After purchasing the identity “fullz”, the more sophisticated markets will then offer the buyer connections to professional forgery operations. Or, they will offer matching documentation as part of the package purchased by the end-user.

This is another area where digital technology has really changed the game. No longer is your local criminal attempting to churn-out passable fake documents using his home computer and printer.

Instead, professional forgery labs produce high-quality documents, utilizing document templates that have been improved over successive generations by using iterative processes to incrementally improve their products over time. In many cases, the forged ID documents produced by such printers are impossible to detect using just the naked eye.

Armed with professional ID documents bearing his or her own picture, containing the identifying credentials of an unsuspecting victim who is a local resident, and armed with many of the details of this person’s economic history, the “casher” is ready to go into business.

“The ability to market oneself as a “digitally secure” organization may be the next great opportunity to gain market share”

Benefits of Reducing the Risk of ID-Related Fraud

In a recent study released by Experian, it was estimated that 2022 saw personally identifying information (PII) hacked at rates that have stayed consistently high to 2021. Consumers have taken notice of the increasing risks to their privacy and a slew of recent surveys have shown that individuals are changing their behavior in response to the frequent stories detailing the vulnerability of their personal information.

In one such study, conducted in 2020, more than 52% of those polled stated they would actively avoid transacting with organizations that had suffered a high-profile breach, such as those experienced by Target, Home Depot and Chase Bank.
While many in the retail industry may view the need to increase security as a burden and a cost-center for the business, forward-looking organizations should see this differently.

The ability to protect your customers’ assets from assault by a steadily improving breed of identity thief offers the opportunity to distinguish oneself in the marketplace.
As customers develop increasing sensitivity to the ID Theft problem they are becoming more averse to doing business with organizations perceived as vulnerable to attack. Thus, the ability to market oneself as a “digitally secure” organization may be the next great opportunity to gain market share in the increasingly competitive market for more customers.

Under the Bank Secrecy Act, institutions have been charged by regulators to actively put into place programs designed to ensure that they are certain of the identity of individuals applying for new credit accounts. Organizations ought to be driven to ensure that they do, in fact, know who a given individual is prior to conducting business with them – whether it be dealings within existing accounts, or during any of a large list of covered transactions.

RetailCo Case Study

RetailCo is a computer and electronics department store that sells computers and consumer electronics through an e-commerce site and through physical store locations operating under the RetailCo banner in more than 15 states. The stores, which reach up to 60,000 sq. ft., stock about 36,000 products across 700 categories, including desktop and notebook computers from major makers the likes of Apple and HP, as well as RetailCo's own in-house brands.

The decision by RetailCo to offer a private label credit card for use in their stores was driven by the same motivations that other retailers share. The opportunity to realize a separate revenue stream from finance fees and interest, as well as the ability to "captive" their customer base into buying from their stores via direct marketing deals and promotions to their card-members. Significant research has shown that such customers continue to engage the retailer at levels far higher than customers who do not own a store-branded credit card. Many different consumer-engagement metrics - such as recurring sales, email opens, website visits, online purchases and others - support this strategy.

In-store, RetailCo customers have been incentivized to open new RetailCo "private label" credit cards through deep discounts offered on the purchases made the first day they open the account. Customers are offered discounts at the cash register, during check-out, if they agree to open a new credit account during the transaction. The program was successful, as evidenced by the large number of new accounts that were created in the 4th quarter of 2014.

However, profits from the successful program were being deeply damaged by fraudulent transactions, with the losses threatening to negate, entirely, any financial benefit the company may have realized from the financing activities. With 12-15 fraudulent transactions per month, at an average dollar value of nearly $3,000 per event, the monthly losses were in the $35,000 - $40,000 range.

Exacerbating the situation is the fact that the actual "hard" dollar-loss from each transaction – that is, the face value of the transaction itself - was typically just a fraction of the total cost to the company of each event.

Making matters worse is the relatively high dollar value of the transactions which were fraudulent. Fraudsters knew which items to target that would be easy and lucrative to resell, so items such as large-screen LCD TV's, laptops and cell phones were among the top items purchased with the fraudulent credit.

Losses by over 3 X

According to the 2022 LexisNexis© True Cost of Fraud℠ Study, conducted annually for the past several years, every $1.00 of fraud loss leads to a total loss of $3.75, after soft costs, such as time spent by accounting, investigations, regulatory filings and other related work associated with a fraud event are considered.

What was causing all the fraudulent transactions?

When confronted with this problem, the Director of Loss Prevention said that what he saw as the common denominator in the majority of the fraudulent events was the perpetrator presented false identity documents, claiming they were the person whose identity they had stolen. He realized that what was needed was some method to empower the stores to authenticate the individuals submitting credit applications.

Identity Authentication via Software

RetailCo conducted an in-depth project to evaluate available solutions to manage the problem. After looking for solutions to this issue, the LP Director determined that, based on what he was aware of, there were no "good or simple processes available to resolve the ID problem".

The most common solutions in the marketplace were variants of different types of software designed to detect anomalies in the credit behavior of the individual submitting an application. However, the Loss Prevention Director said that implementing complex ID authentication and suspicious transaction software offered by numerous vendors was "Too expensive and too complicated". In addition, these fraud detection applications charge on a "per transaction" basis, and the costs continue in-perpetuity.

Software based credit fraud prevention solutions typically involve one or more different methods for fraud detection. The most common software-based credit application fraud prevention method is for the software to present the applicant with a series of questions designed to authenticate identity. Questions such as previous residential addresses, mortgage balances, vehicle loans, universities attended, old phone numbers, etc. These are "public record" data pieces that are compiled into a Q&A exam administered by the store employee. The results are typically able to provide a level of certainty that the person is (or, is NOT) who they claim to be. For many years, these types of screening questions were an accurate technique for identifying individuals.

However, in the modern environment of mass-data hacking and the organization of identity theft as a criminal industry, savvy criminals now will present themselves to apply for credit armed with the information needed to answer many of the questions correctly. Identity "fullz" are often sold in the dark markets with packages that include the answers to many of the most commonly asked questions.

Identity Verification via Document Authentication

A different approach to the identity authentication problem is to look at authenticating the ID document being used by the prospective credit customer.

In financial transactions involving the creation of a new credit account, federal and state legislations require that the issuing company should "know their customer" and conduct an identity authentication. One of the methods that is permitted under regulations such as the Bank Secrecy Act and the Patriot Act is to verify the government-issued ID document presented by the customer as proof of their identity.

In the United States, there are more than 1,100 different variations of ID documents. Considering 50 states, each with multiple different types and design of driver license, as well as state ID cards, alien resident cards, military ID cards, TWIC cards, passport cards, merchant marine ID's, congressional ID's, law enforcement ID's and more. The breadth of different designs and security features is beyond the scope of the ability of a person to be able to reliably verify an ID document without some type of aid.

Equipment is available, today, to enable automatic authentication of identity documents (driver licenses, passports, national ID cards, sate ID cards, TWIC cards, and more) utilizing forensic examination techniques. These devices typically utilize high-resolution cameras to capture images of the document in various wavelengths of light (e.g., infrared, ultraviolet, visible).

FULL-COLOR FRONT

NEAR-INFRARED

FULL-COLOR ZOOMED

For RetailCo, identity authentication was a more acceptable solution

1. It does not require hundreds of employees to be trained on how to use the aforementioned software solutions.

2. Gives options to limit who may be granted access to the sensitive data that may be involved in initiating the software authentication.

3. The PALIDIN Desktop solution is an annual subscription, with no limitations to how many times identity verifications can be conducted.

RetailCo determined that, for their purposes, the ability to authenticate a driver license or state ID card was sufficient, as the vast majority of their clientele would be domestic/US residents. Any customer presenting foreign identity documents, such as passports or non-standard ID cards would be submitted to additional scrutiny and would not be approved for credit using the fast-trak method available at the cash register.

Therefore, PALIDIN Desktop and ID-150 was the ideal solution. The ID-150 scanner is a small, compact device that utilizes a one-step process. It allows a floor-employee to quickly and accurately verify authenticity of the driver license document itself. The employee simply inserts the driver license into the ID-150, and then waits 5-6 seconds for PALIDIN to give a pass/fail result. The ID-150 works only on “ID-1” documents, an international standard sized document that, in the U.S., covers all state driver licenses, State ID cards, U.S. Military ID’s and many other domestic and international driver licenses and national ID cards.

The Director of L.P. chose the 12 hardest-hit stores in his chain to “pilot” the products and prove the concept. The approximate $20,000 purchase price for the equipment and software was roughly equivalent to one average month of “hard-dollar” losses experienced by the stores. Installation of PALIDIN Desktop is just like adding any other program to a Windows-enabled PC. A standard Windows Install Wizard guides the user through the steps to install drivers and database to the PC. After this is done, the ID-150 is simply a plug n’ play device

For enterprise roll-outs, where software is being installed on numerous workstations across numerous locations, the install can be locked-down so that the exact configurations chosen by management are automatically installed on each location. RetailCo used this option, and the installation went perfectly smoothly. Within days of receiving the hardware, all 12 of the initial stores were in-action.

Results

The results were nothing less than terrific. In the words of the L.P. department, everything went exactly as expected. During the first month, on several occasions, fraudulent loans were prevented when the store employee called for the manager to come and speak with the applicant because the ID could not be authenticated. These applicants then fled the location.

Incidences of fraudulent loan applications were halted, completely.

After just two short months, PALIDIN Desktop had already prevented losses greater-than the cost to purchase the equipment. RetailCo management was convinced and decided to expand the equipment to the remaining locations.

At this point, the Director of Loss Prevention decided to approach their credit underwriting bank to ask for their participation in the fraud prevention program. Losses for fraudulent loans were shared between the parties in a manner that was never made entirely clear to FraudFighter.

However, it is clear that both RetailCo and the bank were experiencing losses as a result of the fraudulent loans.

After a great deal of lobbying, eventually, our man was successful in convincing the bank to pay for the 13 ID-150 machines needed to cover the remaining stores. This was achieved by showing the bank exactly what happened before and after the installation of the first 12 ID-150 units.

When compared to the losses that the bank had experienced in the previous 2 quarters, it was clear that in very short-order, the placement of the equipment into the stores would have a positive financial effect on the bank.

RetailCo ordered the final 13 machines. By the next month, the machines were installed and were being used by store employees. The results of the2 month timeframe showed a 54% decrease in fraudulent loan losses during the three month period.

The break-even on the project was realized in remarkably little time. Factoring soft-costs, such as investigations, regulatory filings, employee interviews and other indirect costs resulting from the fraud events into the calculations actually led to the **ROI on the project being achieved in approximately 30 days.**

Conclusion

The modern age of identity theft has fundamentally changed the game for those organizations that conduct business with the public. The sheer volume of personally identifying information being stolen from public and private networks is astonishing,

Perhaps more alarming than the quantity of data stolen is the sophistication of the organized criminal marketplaces that aggregate, package and sell the stolen data to criminals around the globe. For the unprecedented price of only $25, a “casher” can equip themselves with all the information needed to virtually replicate another individual. An additional $100 can supply them with high-quality forged documents, including such items as Social Security Cards, Driver Licenses, and utility bills.

One FraudFighter customer was directly suffering the results of this shifting landscape as the professional identity theft industry targeted their operation.

This consumer electronics retailer had successfully rolled-out a private label credit card to its customer base and was seeing good results from the efforts. However, due to the nature of their industry, they had become victimized as an identity theft opportunity.

The quick and relatively easy credit application process facilitated by the underwriting financial institution, coupled with the retailer’s sale of high-value, highly desirable and easy to resell consumer electronics products made them particularly susceptible to credit fraud perpetrated by individuals with stolen identities and counterfeit credentials.

At the heart of all fraudulent events lies the perpetrator’s belief that they will be able to conduct their crimes anonymously.

This retailer conducted an initial pilot of the PALIDIN Desktop ID authentication and data capture products in 12 of their stores. Within two months, new incidences of ID fraud were halted, completely in the stores thus equipped. This was rapidly followed by a roll-out to the remaining stores in the chain, which the financial institution that underwrites the private label credit card agreed to pay for.

Four months into the full implementation of the solution, fraudulent loans were down by greater than 90%.

While many companies offer solutions for the prevention of ID related loan application fraud, the case study at hand shows the effectiveness of document authentication as a fraud prevention technique. FraudFighter has – for fifteen years – espoused this very theory. At the heart of all fraudulent events lies the perpetrator’s belief that they will be able to conduct their crimes anonymously. Whether it is the presentation of negotiable instruments, the use of credit cards, access to existing accounts, or the effort to open new accounts, the mere act of authenticating the ID document during the transaction strips anonymity away from the transaction.