



SECURE CREDENTIALING DIVISION

Leveraging Best Practices in Customer Proof-of- Identity is Vital to Protect Your Organization from Fraud and Asset Loss

How using Document Authentication during the new account process establishes Trusted Identities and protects financial institutions from fraud.

White Paper

Published:
Sept 2010

The Risk of Identity Theft and Financial Losses Resulting in Fraudulent Transactions

Financial institutions conduct “confirmation” of an identity by scrutinizing application data provided by applicants and correlating the data against third party databases. In support of anti-money laundering and fraud prevention directives a standard copy of the applicant’s passport is taken. While this process is designed to protect the institution from fraud, in reality it creates multiple vulnerabilities that expose the institution to loss.

Financial institutions today simply validate data presented at the time of application. At best, this only confirms the identification and third party searches have been completed -- not necessarily that the person presenting the data is the person they claim to be.

The U.S. Department of Justice spotlights these example cases of fraud related to financial institutions:

- **Central District of California**

A woman pleaded guilty to federal charges of using a stolen Social Security number to obtain thousands of dollars in credit and then filing for bankruptcy in the name of her victim. More recently, a man was indicted, pleaded guilty to federal charges and was sentenced to 27 months' imprisonment for obtaining private bank account information about an insurance company's policyholders and using that information to deposit \$764,000 in counterfeit cheques into a bank account he established.

- **Central District of California**

Two of three defendants have pleaded guilty to identity theft, bank fraud and related charges for their roles in a scheme to open bank accounts with both real and fake identification documents, deposit U.S. Treasury cheques that were stolen from the mail, and withdraw funds from those accounts.

- **Southern District of Florida**

A woman was indicted and pleaded guilty to federal charges involving her obtaining a fraudulent driver's license in the name of the victim, using the license to withdraw more than \$13,000 from the victim's bank account, and obtaining five department store credit cards in the victim's name and charging approximately \$4,000 on those cards.

The Fact About the Current Validation Process Used By Financial Institutions

Financial institutions today simply validate data presented at the time of application. At best, this only confirms the identification and third party searches have been completed—not necessarily that the person presenting the data is the person they claim to be.

Typically, the applicant's proof-of-identity documentation, such as a passport, photo driver's license or a national ID card, is presented as part of the application workflow. Often the document is simply photocopied/ scanned and added to the application. Many times, the data is checked against third party databases—many of which are compiled from publicly-available records that are not available in real-time and often lag by as much as six months.

The software logic behind these services present alerts when data points in the system do not match the data provided by the applicant. When online verification services are used, they provide limited or incomplete information and create multiple opportunities for fraud, including enabling "false positive" identification of an applicant as genuine.

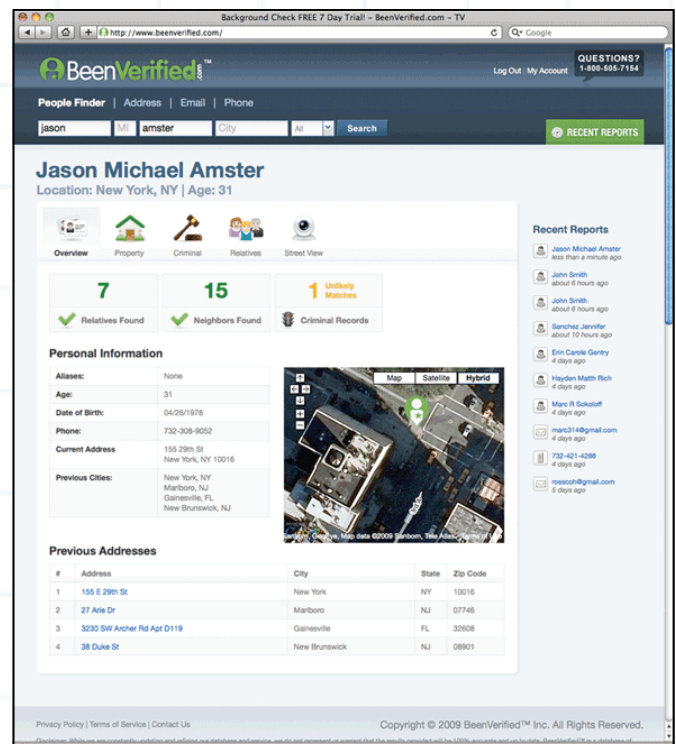
CIFAS Statistics

Statistics released by CIFAS on the 2nd of February 2010, show that in 2009 in the UK that there were 85,000 victims of impersonation and 24,000 victims of bank account take-overs. This represents a 35% and 15% increase respectively from 2008 levels.

Online Verification Services Enable Establishing Fraudulent Identities

Many perpetrators of identity theft often know the person they are purporting to be, allowing them to reconstruct employment histories, mother's maiden names and other security questions often used to validate identification. Even unskilled identity thieves can easily find and replicate the information that is used to "validate" the identity of an individual.

A Google search for a person's full name can result in multiple web links to services that will, for approximately \$25, report the address history and relatives list of the person. Services such as Been Verified allow any individual to pay a subscription fee and run unlimited names through the system to find addresses, relatives' names and criminal records associated with any citizen that has a public persona (such as a phone listing, property or a



criminal record.) From this information they can often reverse-engineer an identity. This information then replicates information the financial institution will find when using systems like Lexus Nexis and other third party verification systems utilizing the same data. In the US, thieves will leverage state privacy laws where driver's license data is not available through verification services; and with driver's licenses being the de-facto identity document in the United States, this presents significant challenges to the financial institutions using these documents as proof-of-identity.

Skilled and resourceful identity thieves can also purchase complete dossiers of alternate identities including seemingly genuine identity documents such as driver's licenses, passports, military IDs and other proof-of-identity documents. These dossiers enable a higher degree of fraud because of their comprehensive nature. In recent years, highly organized crime rings have set up online "dark markets" designed to provide criminals seeking identity information, and those who steal such information, a place to transact business. One such marketplace brought down by international law enforcement in 2009 featured over 1,000 sellers of identity data and featured "banner ads", "monthly specials", "new customer discounts" and other promotional and marketing schemes seen on legitimate e-commerce sites. According to US law enforcement, this one marketplace was responsible for hundreds of millions of dollars of financial institution fraud losses.

Colin Woodcock, head of fraud at SOCA (Serious Organised Crime Agency) in the UK, reported in 28th July 2010 that the agency was now running training courses with the banks to help their staff spot fake foreign passports. SOCA managed to reduce the number of fraudulent documents coming from Nigeria in particular from a flood to a trickle. But he conceded that the problem was likely to reappear in other countries and that this was a crime committed on an industrial scale.

"The Identity and Passport service runs its own passport validation service which has checked a 100,000 UK passports in the last two years. Of these, 1,000 fraudulent passports were detected, saving £4m in prevented fraud. But there is no equivalent service for foreign passports." - <http://news.bbc.co.uk/2/hi/business/8171325.stm>

Did You Know?

A Google search for a person's full name can result in multiple web links to services that will, for approximately \$25, report the address history and relatives list of the person.

"These criminals tend to work on a mass basis. So if you supply hundreds of passports and only one of which opens up a bank account, that is still money to them. They are happy to work on those percentages," said Colin Woodcock, head of fraud at SOCA.

Loss Recovery

Most financial institutions have some form of fraud-related loss recovery capability with a charter to identify the cause of loss and to recover the value. In some cases this is done with internal resources, typically with a loss recovery team that recovers both fraud and default loans as part of their charter. However, sometimes fraud loss in particular is accomplished via outsourcing where a third-party is either paid a success fee for recovered losses, or is paid for court/legal and professional services fees regardless of outcomes.

The High Cost of Recovery

A financial institution with an annual loss of \$50 million dollars may recover 20%.

A financial institution may incur a loss of \$1 million dollars related to fraud, and through an outside service will take the fraudster to court with a cost of approximately \$60,000 for litigation .

Example 1 – Success Fee Model

A financial institution with an annual loss of \$50 million dollars may recover 20%, or \$10 million dollars, for which they pay a success fee of 30%, resulting in recapturing \$7 million of the initial \$50 million loss, or a 14% recovery rate.

Example 2 –Professional Services Fee Model

A financial institution may incur a loss of \$1 million dollars related to fraud, and through an outside service will take the fraudster to court with a cost of approximately \$60,000 for litigation of a criminal case which may or may not result in civil penalties and the successful recovery of funds. The financial institution would carry a caseload of multiple instances of these cases with varying levels of success.

The Challenges in Establishing Genuine Identities

Poor proof-of-identity processes, combined with the high cost and low success rate of fraud loss recovery creates a need for establishing the genuine identity of the individual(s) associated with an account. Yet, commercial enterprises such as banks and major retailers that extend credit face increasing competition and unprecedented pressure to provide immediate gratification, even when performing high price transactions.

Applicant processors -- regardless of whether they are clerks, administrative, branch managers, loan officers or compliance officers -- are rarely, if ever, document forensic experts. While identity document technologies have significantly increased in complexity in recent years, making them much more difficult to counterfeit than ever before, many institutional staff have a false sense of confidence that they can immediately identify a "fake ID". For high value transactions, thieves will invest the money necessary to create a convincing counterfeit document or to alter a genuine ID of sufficient quality that even a skilled person cannot identify it as a fraudulent document.

The production and fraudulent use of highly professional false identity documents is a profitable business for forgers, as well as the fraudsters using these phony identity documents for criminal activities such as banking fraud. Hundreds of thousands of false ID documents have been seized in London in recent years.

Last April, the Metropolitan Police of London, in one North London raid, seized over 2,000 fake passports, identity cards and National Insurance cards, together with security printers, stamps, metallic strips, embossers and holograms.

Since 2004, thirty document factories were uncovered by police in London alone. The number of counterfeit documents in circulation is likely to be tens of thousands of items. Chief Inspector Nick Downing has been quoted as saying, "We could be raiding a factory a day, if we had the resources,"

Without an automated document reader and authentication device, these counterfeit documents will be all too often accepted as proof of identity.

Brazilian Nationals Sentenced to Jail

The UK Border agency announced that three Brazilian nationals were sentenced to a total of five years in jail on Thursday 4 March 2010, for producing hundreds of counterfeit identity documents from flats in London's Bayswater.

Identity Fraud on the Rise

Fraud prevention group CIFAs says that identity fraud -- including identity theft -- is on the rise, with 77,600 cases recorded in 2008, up from 9,000 in 1999.

It cost the UK £1.2bn a year, according to the Identity Fraud Steering Committee in 2008.



Case Study: MAXIM UK 2008 - 2009

MAXIM has obtained convictions for a wide range of immigration related offences, including the conviction of a man for a visa scam whereby many people entered the UK on false documentation; sham marriages where young women, who thought they were going to be models, ended up as part of a criminal operation; and also disruptions of a number of illegal passport factories in London. A joint operation with the Identity and Passport Service uncovered people falsely endorsing passport applications and photographs.

Operation Maxim.	Apr 2007 - Apr 2008	Apr 2008 - Apr 2009
Total Arrests	101	71
Passports seized	1951	1190
Non UK ID docs seized	268	450
Laminators / Embossing machines	20	32
Computers seized	15	16

Source :- The Operation Maxim web page http://www.met.police.uk/op_maxim/

NB. Although the numbers for 2008-2009 have reduced. In 2007, 1500 fake passports were seized in one raid and arrests are less. No UK identity document forgeries are on the increase, due to the purchase and use of specialist laminators and embossing machines.

An Abundance of Identity Documents

In addition to the sophistication of today’s counterfeit documents is the sheer number and variety of valid identity documents in circulation. Not only are there approximately 600 different styles of valid U.S. driver’s licenses and more than 500 different “specialty” driver’s license style (e.g. – “off-road”, “motorcycle”, “commercial vehicle”, etc.) , but there are also a multitude of passports, visas, state I.D. cards, military I.D. cards, work-permit and resident alien cards, diplomat ID cards and a variety of different travel identity documents. Some of these documents may have validity for extended periods, such as the ten-year lifespan of a U.S. passport.

The Automated Document Authentication Approach to Establishing Trusted Identities

Once there is commitment regarding the need to establish the genuine identity of an applicant, best practices dictate not only that data provided on applications be verified, but also the identification documents be "authenticated" as genuine, and that the business process associated with this function is efficient and cost-effective.

Document authentication and identity verification can be conducted at multiple levels to create Trusted Identities. First, authentication of the document itself requires applying sophisticated electronic and optical forensic techniques. Optical analysis can verify the presence of expected security features and proper behavior of the document when subjected to various non-destructive tests. Embedded data acquired from chips, digital watermarks, barcodes, magnetic/optical stripes and printed text is verified and crosschecked to verify integrity and consistency. Security technologies such as digital watermarks are very effective in detecting common ID tampering techniques such as photo substitution. The advantage of this localized approach is that there is no need for the network infrastructure or the time and cost associated with accessing external data sources and dealing with their imperfections (e.g. stale data and gaps in coverage).

The key to implementing an effective Trusted Identity solution is:

1. A comprehensive understanding of all facets of the Document Authentication process
2. The ability to seamlessly integrate the solution into existing business processes using best practices implementation.

Document Authentication

Automated authentication speeds document inspection, which supports faster customer processing and decreases errors due to human limitations such as fatigue, collusion and extortion.

Document Authentication Benefits

- Automatically recognizes any document placed on the glass plate
- Modular design with the ability to implement additional security layers
- Can be combined with biometric identity verification and watch list checks
- Hands-free operation via patent pending brush technology
- Alert resolution tools that provide quick, step-by-step prompts and instructions to help operators quickly and easily dispatch or override
- The system's simplicity and degree of automation means minimal training

In addition, because of the constantly changing landscape that is identity documentation, the solution must also offer an extensive, inclusive document library that is updated on a regular and frequent basis.

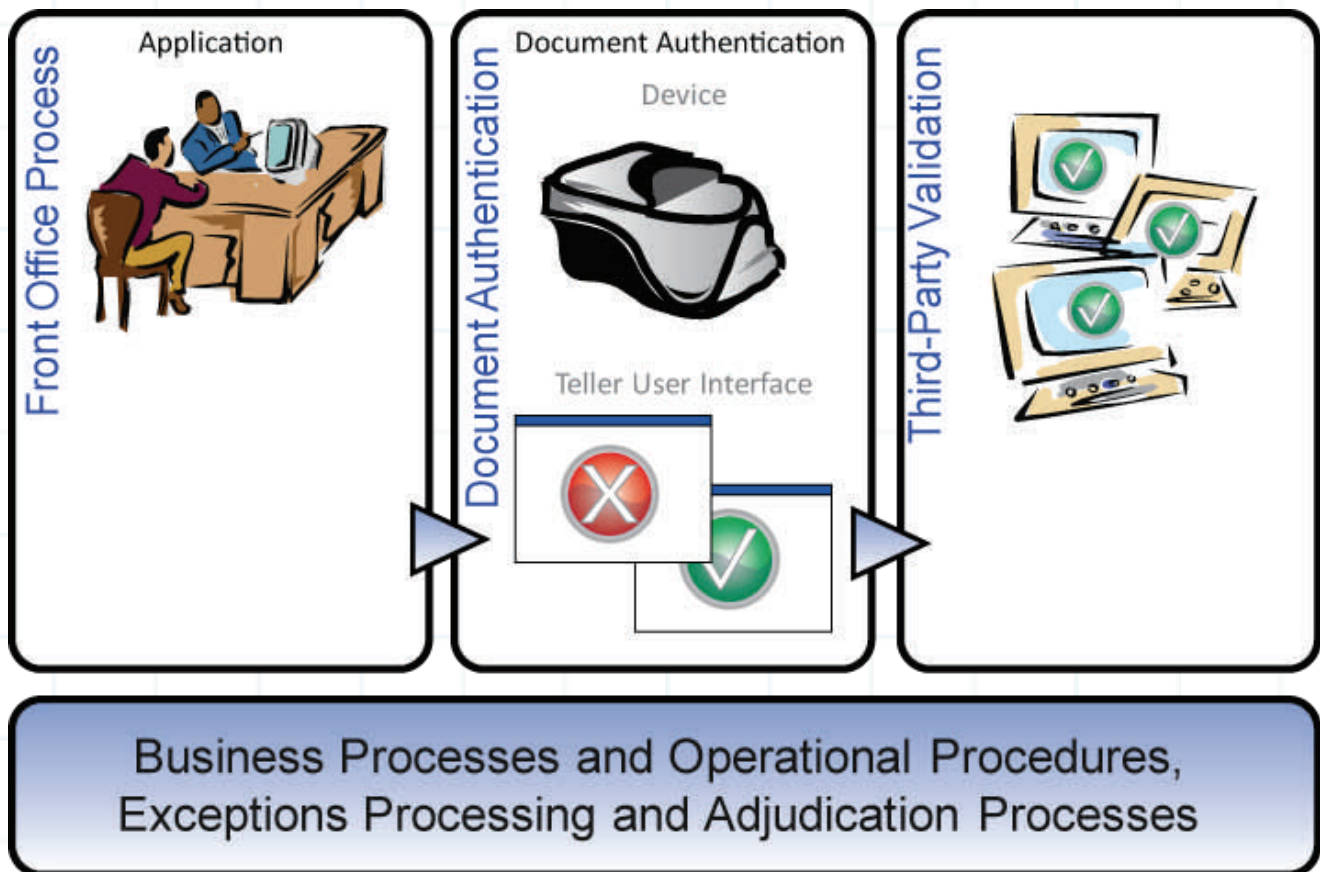
By meeting these needs, complete Document Authentication solutions allow financial institutions to quickly, efficiently, and reliably authenticate the thousands of different identity documents issued in today's environments, and in so doing, to have a high degree of confidence that the applicant is presenting a genuine identity.

A reference model is provided:

Figure 1:

Efficiency & Accuracy

Complete Document Authentication solutions allow financial institutions to quickly, efficiently, and reliably authenticate the thousands of different identity documents issued in today's environments, and in so doing, to have a high degree of confidence that the applicant is presenting a genuine identity.



Business Processes

The business process for authentication demands a high degree of automation to achieve the simplicity and speed required to meet ease of use and customer service expectations, and hence the solution must encompass these considerations:

- Reduce operational overhead through selective application of Document Authentication based on business rules relating to transaction location (focus on high risk areas) and transaction type (new bank accounts or check transactions that exceed a certain value).
- Simple process for performing a Document Authentication transaction. Here ease of use focuses on the ergonomics of the solution. The physical actions associated with processing a document, such as insertion and removal, must be intuitive, flexible and forgiving.
- Simple pass/fail authentication result. Frontline operators should not be burdened with analyzing underlying causes of the result.
- Optimized data acquisition and storage techniques that meet business requirements yet minimize IT network and storage resource utilization. Leveraging configuration options such as document image resolution, image compression quality settings, data transmission during low activity periods, and careful planning of what data is stored under what conditions can result in a total solution that's finely tuned to the financial institution enterprise needs.
- The addition of an audit capability to the tellers' workflow to mitigate risks associated with teller collusion.

Benefits

- Reduce operational overhead
- Simplify processing
- Easy to understand pass/fail results
- Optimized data acquisition and storage techniques
- Audit capabilities



Exception Handling

Moving from a reactive (after the fact) model to a proactive (preventative) model has benefits, but also presents a few operational challenges best addressed with an adjustment to current business processes.

Business rules can be established to institute front-line exception handling procedures such as repeating the document scan to ensure proper insertion, requesting alternate forms of identification, asking security

questions, etc. Many times, the handling of remaining authentication exceptions is best left to skilled staff dedicated to performing this function. Larger organizations may have trained people at each site, or may employ a centralized internal function. The next option is to initiate a remote adjudication action, and while this further extends the length of the transaction, for high value transactions it is the best way to protect the financial institution from loss.

The process for responding to legitimate authentication alerts may also vary depending on financial institution business practices or State law. A person presenting a fraudulent document is not necessarily trying to commit a fraudulent financial transaction. The fraudulent document may have been obtained to establish illegal residence and gain employment, yet the bearer may now be fully integrated into the country and pose no threat of illicit financial transactions other than using an assumed name and/or a forged document.

However, holding and using a forged identity document is a criminal offence. A solid business process will have an approach that covers the most likely scenarios to a degree relative to the potential risk, and those risks may be measured differently by different financial entities.

Exception Handling

The process for responding to legitimate authentication alerts may also vary depending on financial institution business practices or State law. A person presenting a fraudulent document is not necessarily trying to commit a fraudulent financial transaction.

Best Practices Tie the Applicant to Their Identity Documents to Create a “Trusted Identity”

It is very possible for an intelligently organized criminal entity to obtain extremely large profits from fraudulent financial activity.

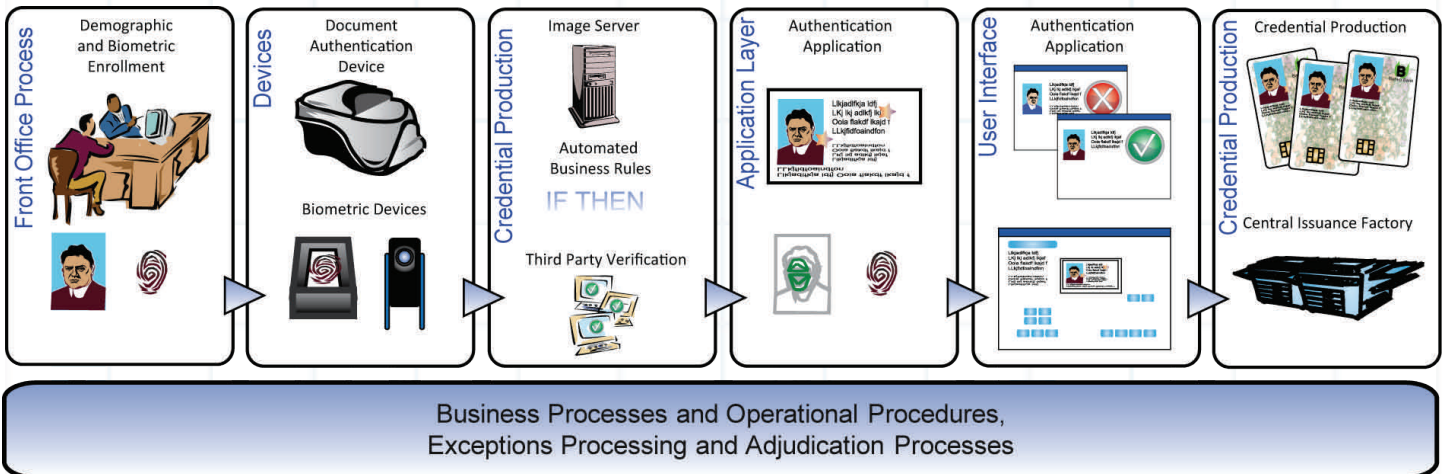
For financial institutions that conduct high-worth transactions, a means of tying the applicant to their identity documents provides significant value, including countermeasures for large-scale fraud plus the ability to create a differentiator aimed at obtaining high-net-worth individuals and institutions.

One means of tying the applicant to their identity document is to use biometric enrollment at the time of establishing a new account. In this way, a biometric is associated with an authenticated document, which is then established as proof of Trusted Identity with the account. The aforementioned solution is thus expanded to include biometric enrollment, the optional issuance of a specialty ID document, and the use of biometrics at a later date in order to authorize a transaction. (See “Your Competitive Differentiator” section)

When Handling Exceptions, the Business Process Must Encompass These Considerations:

- A management function for processing authentication exceptions provides of response times that can be tailored to business needs so frontline operations, hence customer service levels, are not adversely affected.
- Many commercial operations lack a local secondary support infrastructure so there is an increased dependence on a centralized function, possibly an outsource service provider, for dealing with authentication exceptions.

Figure 2:



This vision of business value for the financial services industry is a complete solution available today from L-1 Identity Solutions.

- Biometric and demographic enrollment can be seamlessly tied into the front office applicant processing workflow.
- Biometric images and demographic data are then stored in the server, where automated business rules parse the data and bounce appropriate fields against third party databases such as Choice-Point, LexisNexis, Trillium or others of choice.
 - Additionally, images of scanned documents can be retained securely for future needs such as auditing or forensic investigation.
- An optional credential/ID can be generated as a trusted token, and the biometric can optionally be stored on the card for future authentication.
- The Document Authentication solution then verifies the authenticity of the proof-of-identity documents presented at the time of application, and through its user interface (available in multiple languages) then provides a pass/fail result.
 - Failures can be adjudicated to a second tier manager as described previously
- Devices are then used to authenticate the credential/ID and/or the biometric at the time of future transactions (such as large withdrawals, significant loan activities, etc. according to the business needs of the financial institution.)

- The enrollment can be enhanced to facilitate the development of a private “loss prevention” biometric database that includes information and matching capabilities for barred patrons, known criminals, perpetrators of slip-and-fall lawsuits, etc. In the future, this system could be expanded to a fraud investigation network, allowing financial institutions to share this information.

If any of the above results in a suspect identity, the financial institution can request the applicant to provide additional documentation prior to proceeding with the application process, or may implement a business process that delays processing and notifies law enforcement. Unfortunately, some institutions may opt to forego the third party database functionality, and it's associated per-transaction cost, in lieu of Document Authentication, which has no transactional cost burden and provides a high degree of certainty that the credential is genuine.

Because of the robust nature of the data gathered, financial institution CRM systems can be bolstered, depending on Privacy Laws and local business practices, by adding data collected from the scanned documents to the applicant's digital portfolio.

This level of Trusted Identity, while more complex initially for the applicant, allows the financial institution to competitively position

themselves as offering a higher degree of identity protection for the consumer. Whether a private banking scenario, a high-net-worth transaction, or other high-risk transaction, the benefit to both the financial institution and the individual is clear: Only a Trusted Identity will be able to establish the account, and only a Trusted Identity can then conduct transactions associated with that account. No other business process is as secure.

A Trusted Identity

Because of the robust nature of the data gathered, financial institution CRM systems can be bolstered, depending on Privacy Laws and local business practices, by adding data collected from the scanned documents to the applicant's digital portfolio.

This level of Trusted Identity, while more complex initially for the applicant, allows the financial institution to competitively position themselves as offering a higher degree of identity protection for the consumer.

Whether a private banking scenario, a high-net-worth transaction, or other high-risk transaction, the benefit to both the financial institution and the individual is clear:

Only a Trusted Identity will be able to establish the account, and only a Trusted Identity can then conduct transactions associated with that account. No other business process is as secure.

From Capital Budgets to Discretionary Spending

A general tendency to scrutinize capital budgets and minimize larger capital expenditures has led to an historical bias towards online verification services, where the expense is incurred on a “per transaction” basis with little or no front-end cost. Such transaction-based solutions may appear at the surface to be more cost effective relative to the capital investment required to acquire a genuine “Document Authentication” solution.

Financial institutions evaluating the available options for proof-of-identity solutions should build a business-case which justifies the investment needed by utilizing a comparative return-on-investment model.

Online verification solutions are a recurring expense. The subscription model may include monthly fees, per-seat license fees and transaction costs ranging from as low as pennies-on-the-dollar to more than \$3.00 per transaction depending upon the level of detail, the volume of searches conducted, the service provider, and the nature of the search.

In building a business case for establishing Trusted Identities, financial institutions should consider the annual cost of conducting per-transaction identity verifications, and then forecast this cost every year, with appropriate growth rates, for the duration of whatever evaluation period is being examined. For appropriate comparison purposes, the analysis should consider the cost of using online verification for all the areas of the operation which either currently or in the near future may require proof of identity, such as new account openings, wire transfers or other covered transaction types requiring customer identity verification under BSA, FACTA and CIP rules.

The comparative cost model should additionally consider the fact that the Document Authentication System, implemented at the front-end of each of the transactions requiring proof-of-identity, will prevent substantial expenses incurred, first, from processing fraudulent or incomplete transactions, and second, from incurring “soft costs” (e.g. investigations, audits and filing of reports) associated with such transactions.

Considered in entirety, the total cost of ownership (TCO) of the Document Authentication solution, which is a hardware/software purchase enabling unlimited Document Authentications, will, over time, prove to be considerably lower than the perpetual per-transaction fees associated with online verification services.

A recent TCO analysis by a financial institution showed that the costs of the Document Authentication solution was significantly less than the long-term cost of conducting online verifications. Additionally, costs associated with online verification aren't typically addressed until after the purchase decision, such as branch set-up costs that may require structured financing, or the operational costs of manual entry of ID data into branch systems that could otherwise be automated with Document Authentication.

Subscription Model

Online verification solutions are a recurring expense. The subscription model may include monthly fees, per-seat license fees and transaction costs ranging from as low as pennies -on-the-dollar to more than \$3.00 per transaction depending upon the level of detail, the volume of searches conducted, the service provider, and the nature of the search.



The Bottom Line is the Bottom Line

Ultimately, the real and quantifiable value of Document Authentication is the tens of millions of dollars it saves organizations by virtually eliminating losses related to processing accounts associated with fraudulent identities. Applicants attempting to open accounts or obtain credit with fraudulent ID documents are unsuccessful in their attempt, and are either reported to law enforcement or will seek alternate financial institutions that do not perform identity authentication. Often times, this removal of the threat is enough to make the case for investing in the technology because the amount each institution loses each year related to identity theft is tracked as a performance metric.

Your Competitive Differentiator—Creating New Business

In addition to Document Authentication protecting financial institutions from fraud, it can also create a competitive differentiator. Document Authentication can be extended beyond the application process to the transaction process by implementing a business process that requires proof of identity for high value transactions. These can be customized to a financial institution's needs.

Marketing these Trusted Identity Services to high-worth individuals as a means of protecting their assets from fraud creates a significant

The Truth

Ultimately, the real and quantifiable value of Document Authentication is the tens of millions of dollars it saves organizations by virtually eliminating losses related to processing accounts associated with fraudulent identities.

Example – Private Banking

A financial institution can create an additional layer of security for high-worth accounts by establishing optional business processes associated with private banking. Transactions could be secured for large withdrawals by requiring Document Authentication at the time of withdrawal at a branch location.

Example – Biometric Authentication

Fingerprint or facial biometrics can be added to the system by having high-worth individuals biometrically enroll with your financial institution. A biometric match (via an in-branch camera or fingerprint device) then authorizes the transaction.

competitive advantage over institutions that do not provide this services — while simultaneously ensuring that fraudsters take their fraudulent business to other institutions.

Why L-1

In the context of financial institutions, identity validation says "this data is legitimate", Document Authentication says "this document is genuine" and the business process, which can be executed at varying degrees of complexity says "this verified data plus this authenticated document plus this physical applicant conducting the transaction combine to create a Trusted Identity".

Now, more than ever, large institutions and government entities need solutions that safeguard our security, protect against identity theft and fraud, and keep business moving. These solutions must not only be technologically sophisticated and easy to use, they must also be implemented using best practices that allow them to be seamlessly integrated into existing business procedures. L-1 Identity Solutions is the only company that can provide the technology, the expertise, and—most importantly—the depth and breadth of experience necessary to achieve the objective of creating Trusted Identities for applicants as a means of protecting financial institutions from fraud related to fraudulent identities.

Creating Trusted Identities

L-1 Identity Solutions is the only company that can provide the technology, the expertise, and—most importantly—the depth and breadth of experience necessary to achieve the objective of creating Trusted Identities for applicants as a means of protecting financial institutions from fraud related to fraudulent identities.

Protecting Your Organization From Identity Theft

Now, more than ever, large institutions and government entities need solutions that safeguard our security, protect against identity theft and fraud, and keep business moving.

These solutions must not only be technologically sophisticated and easy to use, they must also be implemented using best practices that allow them to be seamlessly integrated into existing business procedures.

About L-1

L-1 Identity Solutions, Inc (NYSE: ID) protects and secures personal identities and assets. With the trust and confidence in individual identities provided by L-1, international governments, federal and state agencies, law enforcement, and commercial businesses can better guard the public against global terrorism, crime, and identity theft fostered by fraudulent identity.

- L-1 has deployed over 10,000 Document Authentication systems world-wide including banking, retail, border control and state government.
- L-1 has identified and protected our customers from at tens of millions of dollars in identity-related retail fraud alone.
- L-1 provides products and services that enroll and enable more than 100 million personal identification documents a year including 80% of U.S. driver's licenses representing more than 200 million motorists in over 40 states the District of Columbia.
- L-1 is also the provider of the U.S. Passport and U.S. Passport Card, enhanced driver's licenses for WHTI-compliant border crossings, as well as credentialing and ID solutions in more than 20 countries worldwide.
- L-1 systems enroll millions of applicants annually, and runs more than 600 billion facial image comparisons nightly; more than any other government or non-government entity world-wide.
- L-1's Document Authentication solution includes more than 2,000 types of identity documents used world-wide
- L-1 is unparalleled in identification management leadership and total solution design acumen.
- L-1 has established a network of over 135 surveillance operators located in the United States, Canada, Puerto Rico, Bahamas and Aruba to help quickly identify suspicious patrons.

L-1 Identity Solutions

- Leader in document authentication and scanning world-wide, totaling more than 10,000 systems.
- Proven End-to-End solution provider supporting multiple technologies.
- Offers a one-stop-shop with a unique combination of security, technology and systems integration experience.
- Personalize more than 100 million secure credentials annually.
- Produce over 2/3 of U.S. drivers' licenses.