FRAUD FIGHTER™

WHITEPAPER

AN OVERVIEW OF IDENTITY AUTHENTICATION

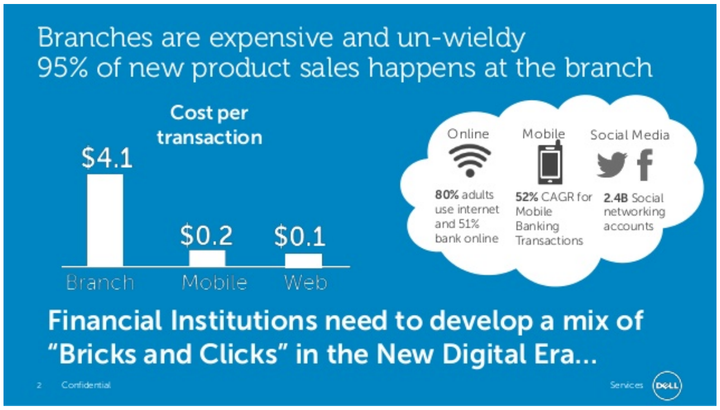
HOW TO MAKE SURE PEOPLE ARE WHO THEY SAY THEY ARE QUICKLY, EASILY, CONFIDENTLY

Sean Trundy,
COO

Table of Contents

Balancing Convenience and Trust in Customer Transactions

Consumers want to transact with your company quickly and efficiently, with minimum trouble, from anywhere they may be. For most companies that provide high trust services and products, the challenge lies in accommodating this customer demand for convenience while still maintaining compliance and minimizing the risk of losses that may result from fraud.



Branches are expensive and un-wieldy
95% of new product sales happens at the branch

Financial Institutions need to develop a mix of "Bricks and Clicks" in the New Digital Era...

2 Confidential Services

Organizations across almost every industry face a rapidly changing environment in which the choices are simple – either adapt to the modern paradigm of mobile and online transactions, or become fatally incapable of competing with others in your industry who do. Organizations 'move to online transactions is not only driven by the need to satisfy customer demand, but also by the requirement to reduce expenses and remain cost-competitive in the marketplace. Online transactions typically cost less than half of an in-store transaction, and in many cases can cost 80-90 percent less. Thus, companies that do not move to this transaction model put themselves at remarkable disadvantage.

Some organizations may require that transactions be conducted in-person at a brick and mortar location so that they can ensure people are who they claim to be. While this may be a one-time process, such as establishing a new account - or an ongoing requirement, such as verifying identity when a client conducts transactions that have regulatory compliance issues - it may be in direct conflict with consumers' desire to conduct transactions not only in-store, but also from remote locations via the internet or through mobile applications.

You need high confidence in a person's individual identity so that you can provide engaging and efficient customer experiences, but where do you draw the line between being easy to work with and managing the risk that your customers may not be who they claim to be? And how do you ensure a frictionless customer acquisition or transaction process while protecting your company from fraud and loss?

SecureIDCloud™

FraudFighter's *SecureIDCloud*™ suite of identity authentication solutions provides identity assurance everywhere identity matters. With our solutions, people can easily prove that they are who they claim to be, with a high degree of trust, wherever they are, and at any time.

At the core of FraudFighter's strategic approach to the identity trust issue lays the fundamental belief that the first step in establishing trust is to authenticate the credential of the individual. In most cases, this will be a government-issued identification document, such as a passport, national ID card or driver license. Once this has occurred, organizations can choose to then utilize authenticated personally identifying information (PII) to enable additional value-added applications. Examples might include enrolling their client into a biometric credentialing system, auto-filling forms and applications, verifying age, running individuals against watch lists, and more.

The identification process can be adapted based on the level of assurance required – allowing the right blend of technology and process to manage identity risk while being cost-effective and providing the great customer experience people have come to expect in the modern digital age.

Authentication of identity documents may be performed at stationary workstations (e.g. at the cashier or teller window), or on smart mobile devices, e.g. phones and tablets. Enterprises may design authentication processes that utilize both on-site and mobile authentication procedures, both of which would be hosted on a common platform.

The *SecureIDCloud*™ platform enables fast, reliable verification of individual identities. It is a cost-effective, scalable software solution that is able to use one or more identity characteristics, including biometrics (i.e., face, fingerprint, and iris), authentication of documents (i.e., driver licenses and passports) and verification of data to establish identity. The solutions scale to your needs and can be configured for identification capabilities on-demand, everywhere identity matters.

Example capabilities include:

- Mobile or on-site enrollment of new customers based on authenticating their proof-of-identity documents
- Make sure employees are who they say they are based on their proof-of-identity documents; e.g. I-9 compliance
- Biometrically enrolling new customers
- Identifying customers with our hosted 1:N biometric matching solution, in our cloud or in your own private instance
- Biometrically verifying the identity of people on a 1:1 transactional basis can be done in real-time and can scale to any volume and throughput requirements
- All of our core capabilities are available as REST APIs for your own development or for implementation by third-party developers

Our hosted solution helps to reduce your costs for systems, hardware, support and maintenance, while eliminating or reducing the need for your own data center operations. We are continually adding new technologies and capabilities to our SaaS and our API catalog, and because they are available as a service, they are immediately available upon release.

IDentity Authentication Products

FraudFighter provides a multi-tiered approach to authenticating client credentials. This allows clients to target the appropriate solution to the appropriate risk exposure and business use-case requirements of each unique potential customer interaction.

Ultra-Violet Point of Sale Scanners

At the decidedly low-technology end of the scale is the concept of verifying credential documents by using Ultra-Violet (UV) light. FraudFighter is an 18-year leader in this industry, and has provided UV verification equipment to global clients such as Bank of America, Wells Fargo, Chase, Macy's, Kroger, and hundreds of other leading organizations.

Low cost. Easy to use. Very easy to implement. Effective. These are the characteristics in favor of using UV detectors. The machines can be installed, and employees trained, by a store-level manager within minutes, and there is no need to connect to the internet, install software, or otherwise involve numerous departments to get them operating.

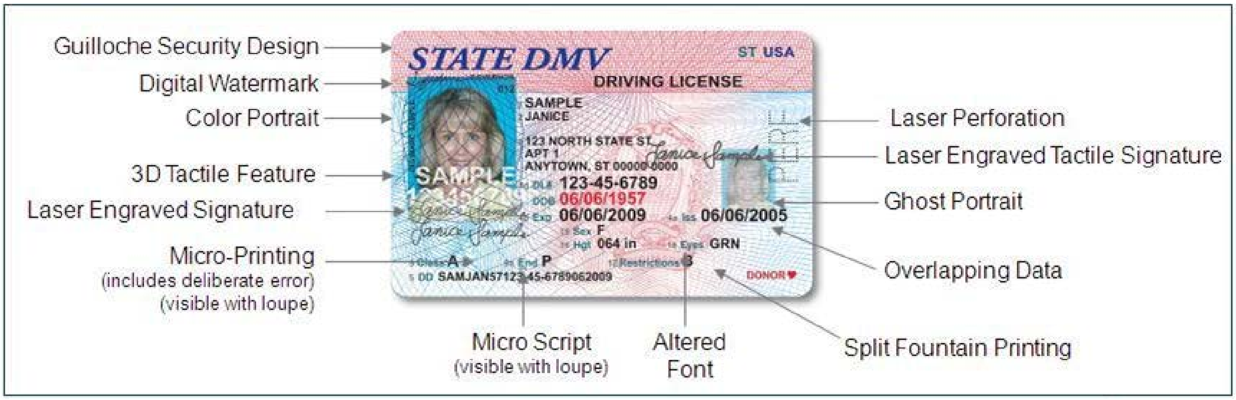
The offsetting downsides to using UV detection scanners are that, because the devices are so simple, they do not provide complex business use-case benefits, such as capturing and syncing personally identifying information to business applications, or providing a record of the authentication to ensure employee compliance with work rules. Also, although effective, UV lights are by no means infallible, and it is possible that advanced-level organized crime rings may be able to produce fraudulent ID documents with UV security features on them. Thankfully, this is still a relatively rare occasion at this time.

UV Scanners can be either stationary, or portable.

Point-of-Sale ID Document Data Capture and Authentication Scanners

These devices are a major step-up in terms of technological sophistication compared to UV detection scanners. The general principle is to utilize a specialized ID scanner device to take high-resolution images of ID documents. Such scanners are produced by a number of different vendors. The images are often taken under different wavelengths of light, including UV and infra-red (IR), as well as standard visible light. In addition, digital data that may be stored on identity documents in a variety of different mediums is read by the scanners. RFID chips, magnetic strips, barcodes, digital watermarks, B900 "MRZ" content and other sources of data are collected, collated and compared.

ID-150 Document Scanner



Once the data is collected, software-based authentication libraries go to work comparing the images to their databases of known design features. The software verifies that the design elements and manufacturing methods of the document meet the unique specifications as defined by the agency that issued it.

Different vendors of the authentication libraries make different options available for the IT architecture of these solutions. Also, some vendors enable add-on functions, such as the ability to conduct facial-comparison of the person holding the document to the image on the document. Also available as a part of a modular identity management system are biometric enrollment programs or watch-list database lookups.

Accessing the Document Library
The simplest form of an authentication software installation would be to load the authentication library onto a Windows-PC workstation at the location where authentications must be conducted. This creates stand-alone solutions that need-not be connected to a network or have any access to the Internet.

Also possible is a “distributed” model. That is, a single installation of the document library on a server managed by the client would allow for multiple document scanner units, each attached to a point-of-transaction workstation, to have the documents scanned at a local workstation, but tested by the software on the server.

A third option is to use a cloud-based version of the authentication library. Under this scenario, document scanners can be attached to a thin-client computer at the point of transaction, and the images and data are processed remotely by a cloud-based version of the authentication library.

Mobile Identity Authentication

Many potential business-cases point to the desire to have an identity authentication solution available as a mobile application on a smart phone or tablet. In some cases, it simply isn’t feasible to have a stationary device, tethered to a PC, available at the location where authentications must occur. In other cases, it may be desirous to have a client that is

not in your physical store or branch location conduct an identity authentication wherever they are – which might be in their home, at a hotel, or even walking on the street.

Mobile IDentity Document authentication is a challenging task. In the United States, alone, there are more than 1,200 different valid types of identity document. The task of recognizing and authenticating such a large variety of documents requires significant knowledge about the documents themselves and what to look for.

Authentication with a mobile device must rely on images captured by the cameras that most iOS and Android phones now include that are of sufficient quality and clarity to allow for deep-pattern-matching. This process – deep pattern matching – compares ID images to a comprehensive identity document library with detailed information about the design of each different type of ID. FraudFighter is partnered with the leading document library companies in the world to provide these solutions.

Frequently Asked Questions

How are ID documents authenticated?

Authentication occurs in a number of ways, depending upon which solution is being utilized. With a UV device, the user visually observes the presence of a fluorescent security feature, and subjectively determines that the document is good or bad.

With point-of-sale scanners, the process is highly complex, and produces the most accurate results. Data from any available digital storage medium on the ID is read and cross checked against the other sources and against the optical character recognition (OCR) information read from the front of the license. Software ensures that all different data-points are in agreement.

Deep pattern matching is utilized to compare high-resolution images of the ID document obtained in different light sources against the document library to ensure that actual document production processes and procedures were followed. This process also verifies numerous – in some cases dozens – of security printing techniques, such as micro printing, watermarking and more.

The FraudFighter IDApp reads the barcode, and then compares the data to the Enhanced Security Feature (ESF) data. Note that not all ID documents have barcodes and/or an ESF. In this case, the front of the license is imaged and a deep pattern match is conducted that is similar to that conducted with the point-of-sale scanner, with the exception that only white-light (visible) images are used for authentication.

What happens to the personal data?

As a leader in fraud prevention, we take the safety and security of personal identity data very seriously. We have observed the steady increase in the instances of mass data hacking, and have researched and reported frequently about the sophistication of the criminal marketplaces that have arisen to capitalize financially on the stolen data. For this reason, we are committed to absolute security on any data that is managed by our systems.

Every process we design which in any way touches personally identifying data is built with data security in mind. Several overriding principles guide us in this approach:

1. Only capture and process necessary data. Prior to communicating any personal data, we ask "what is the minimum data necessary to achieve the stated goal". We then design our integration processes to only synchronize the data that is necessary
2. Move the data the fewest possible number of times. Some of the add-on processes required to achieve the expanded benefit of authenticating an individual will require that data be moved between different applications. In designing custom configurations for clients, the fundamental design will be driven by the goal of minimizing the number of times this is required.
3. Utilize industry best-practice security standards. Security vulnerability testing is conducted constantly. Our membership in Cloud Security industry groups allows us to keep an as-current-as-possible awareness of new information, vulnerability and hacking incidents occurring in the industry and new developments in the virtual and cloud application marketplace.

What if we don't want employees using their own smart phones?

Many organizations are quite comfortable with the "bring your own device" mentality; however, we realize that this may not be appropriate for your organization, or for the specific purpose in mind in this instance – e.g. capturing images and data from ID documents.

For this reason, FraudFighter is able to provide dedicated mobile devices to clients with our IDApp application pre-installed at very reasonable prices.

Partners in Technology

FraudFighter partners with several of the leading global suppliers of identity authentication tools and equipment to deliver a full suite of solutions.

MorphoTrust

MorphoTrust, a part of international conglomerate Safran, is a 40-year veteran of the identity and credentialing industry. Among other things, MorphoTrust has inherited the legacy businesses of both Polaroid and Visage, and is one of the leading suppliers of secured credential documents in the world to government and commercial clients. In the United States, they produce 80% of the identity documents used by US Citizens and legal residents.

AssureTEC

AssureTEC is the manufacturer of the AssureID database, a complex library of global identity documents used to conduct document authentications. AssureID can integrate with ID document scanners from a variety of providers, such as ARH and Desko, and uses the images and digital data captured from ID documents as the basis for determining their authenticity.

AmazonCloud™

Amazon is one of the world's largest providers of cloud data storage and management services. FraudFighter partners with Amazon for the delivery of cloud-based business solutions that enable the central processing and collection of personally identifying information in a secured environment built and monitored by a global leader in this rapidly evolving space. This data is readily available for integration to core business software systems.

RackSpace

Rackspace is a leading provider of cloud application development, secure data monitoring, and data integration solution development. FraudFighter partners with Rackspace to provide customizable web-based applications for the collection, analysis and integration of data within a secure environment, whether cloud based or self-hosted by the end-user.