FRAUD FIGHTER™

(800) 883-8822

Thought Leadership Series

Customer Credentialing in Financial Institutions

How Reducing the Risk of ID-Related Fraud can differentiate your Financial Institution, Increase Market Share, and Decrease Losses

Sean Trundy, C.O.O.

FraudFighter Products

1/5/2015

Contents

About the Author

Sean Trundy is a 12-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 100 different banking organizations, including Fortune 100 giants such as Wells Fargo, Bank of America, Citizens, Regions, Chase and more.

Customer Credentialing in Financial Institutions

How Reducing the Risk of ID-Related Fraud can differentiate your Financial Institution, Increase Market Share, and Decrease Losses

The deluge of news stories in recent years regarding stolen personal data and the increasing issue of identity theft highlights a problem that financial institutions cannot afford to ignore. In a recent study released by Experian, it was estimated that more than 110 Million pieces of personal data were bought and sold in the first 9 months of 2014, a greater than 300% increase from just two years earlier. 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 September of 2014, more than 50% 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.

Brand Insight

"The ability to market oneself as a "digitally secure bank" may be the next great opportunity to secure market share in the financial services industry"

While many in the financial services 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. This is a modern play on an old concept. Throughout the centuries one of the primary services offered by banks has been the safe-keeping of customers' assets. While in the past this may have been demonstrated by installing impressive bank vaults and designing impenetrable buildings, in the modern age, the act of securing client assets is represented by sophisticated digital defenses.

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 bank" may be the next great opportunity to secure market share in the financial services industry.

Among the opportunities available in this burgeoning area is the concept of "credentialing" ones' customers. Generating a unique credential for each customer that is based on a highly secure biometric process is a certain way of ensuring that fraudsters will not be able to access customers'

accounts and assets.

Under the Bank Secrecy Act, financial institutions have been charged by regulators to actively put into place programs designed to ensure that they are certain of the identity of individuals with whom they are transacting. However, such regulations are ambiguous and do not define with precision just what it means to "Know Your Customer". As a result, many in the industry have opted to utilize the most commonly available method – achieving a "confirmation" of identity in order to come into compliance with the regulations. This practice of accepting the default solution fails to address the customers' best interests. Financial 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.

Online Verification Services Enable the Establishment of Fraudulent Identities

Currently, most financial institutions conduct confirmation of an identity by scrutinizing application data provided by applicants and correlating the data against third party databases. While this process is designed to protect the institution from fraud, in reality it serves to create vulnerabilities that expose the institution to loss. Simply validating identification information presented at the time of an application at best does nothing more than confirm that the data is real -- not that the person presenting the data is the person they claim to be.

Typically, the applicant's proof-of-identity documentation, such as a driver's license or passport, is presented as part of the application workflow. These documents are often simply photocopied or scanned and added to the application. Next, the data from the ID documentation 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. Such database verification services are designed to alert the institution when data in the fraud detection system does not match the data provided by the applicant. When such verification services are used, they create multiple opportunities for fraud – in some cases, enabling a "false positive" identification of a fraudulent applicant as genuine.

Many perpetrators of identity theft often know the person whose identity they are stealing, 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. From this information they can often reverse-engineer an identity, effectively replicating the information a financial institution will find when using third party verification systems.

Identity Theft as an Industry

In recent years, incidences of mass-data breaches have created a glut of personally identifying information on the dark web where such data is bought and sold. Markets such as Agora, Evolution and Silk Road 2 serve as aggregators of data stolen by hackers. Utilizing modern database management tools, these marketplaces run data matching tools and filters and are able to assemble information about individuals that may have been stolen from a variety of different sources. These are assembled into profile "fulls", which are sold – often in bulk – to criminal organizations around the globe.

These dossiers enable a higher degree of fraud because of their comprehensive nature. The full profiles often contain all of the information required to answer the third-party database questions, and may also contain passwords, pin #'s and other important data. Identity thieves can also purchase seemingly genuine identity documents - such as driver's licenses, passports, social security cards, military IDs and other proof-of-identity documents – from professional forgery operations selling on the same dark markets where the identity data is being bought and sold.

Armed with high-caliber counterfeit identity documents, a "full" profile of a stolen identity, and answers to many of the questions that 3rd party databases might ask, the fraudster is now armed and ready to come to your branch. They may simply be looking to open an account they can use to launder funds. Or, they may have detailed information sufficient to allow them to apply for a home-equity line of credit against real estate owned by the person whose identity they have stolen. Regardless of the intended fraud, most institutions will not be properly equipped to detect the false identity, and are likely to process the transaction.

Credentialing – a New Paradigm in Securing Customer Assets

Faced with a criminal element that has adapted technology at alarming rates, financial service organizations are left with no choice but to increase their defensive capabilities. One cannot overstate the reputational damage that might occur to the institution should an organized crime ring discover a vulnerability and make repeated successful fraudulent transactions against the assets

owned by customers of the institution. Not only will the institution suffer in the public opinion, but the direct financial losses from fraud can be substantial, and if proper procedures were not followed, fines and penalties assessed by federal and state regulators could be significant.

In order to avoid this potentiality, banks and other financial service companies have the opportunity to create a process that will allow them to be certain that any individual transacting with them is, in fact, the person they claim to be. The means to achieve this is enabled through a two-step customer credentialing system.

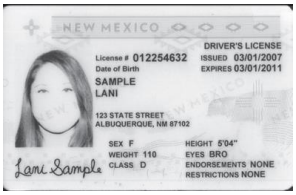
Step 1: Verify the Identity Document

The first step in knowing your customer is to submit their proof-of-identity document to a high-level authentication test. In the United States, alone, there are more than 1,100 different currently-valid government-issued proof-of-identity document designs. Considering 50 states and 4 territories, each with multiple different driver license and ID card types, passports, passport cards, US permanent residence cards, military ID's, congressional ID's, TWIC cards, and a host of other eclectic documents issued to both citizen and non-citizen individuals as proof-of-identity, the number of legitimate documents is far too great for any person – no matter how well trained – to be able to verify ID documents without help.

Factor-in the recent technological innovations being utilized by organized crime rings, with their access to accurate personal identity data and professional forgery rings, and what you end up with is exposure to genuine risk of accepting fraudulent documents.

Equipment is available, today, to enable automatic authentication of documents utilizing forensic examination techniques. These devices typically utilize high-resolution cameras to capture

FULL-COLOR FRONT



NEAR-INFRARED


FULL-COLOR, ZOOMED

images of the document in various wavelengths of light (e.g., infrared, ultraviolet, visible).

They also “read” data stored in various digital formats on the document, whether in magnetic media, barcodes, near-field RFID chips, or digital watermarks. The images and the digital data are than compared to a database of “known” design and manufacturing elements for each document type, and a pass/fail grade is assigned.

Step 2: Capture a Biometric Identifier

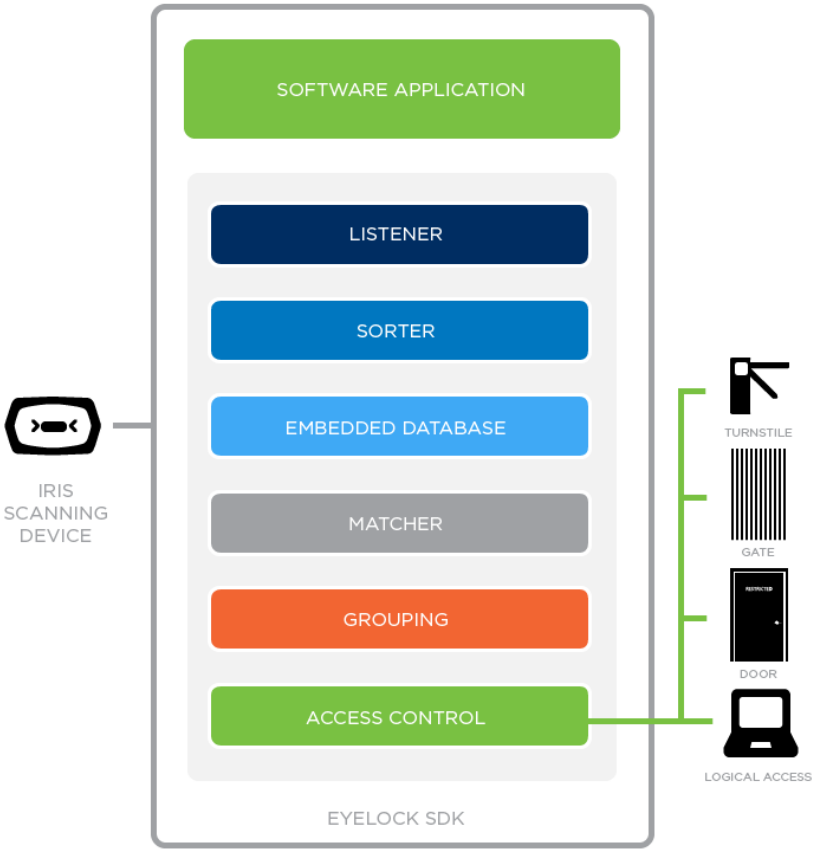
Once the proof-of-identity document has been authenticated, the next step is to enroll the customer into the customer database using a biometric identifier. It is vital that this step occur at the same time that the ID document has been authenticated to ensure that the person presenting the document is the same person who is credentialed using the biometric identifier.

Although there are several different methods of obtaining a biometric identifier, recent advances in technology have made the capture of an iris scan the most attractive option among the available solutions. Iris scans can be “passively” captured, meaning the individual need not touch any equipment, as might be necessary with, for example, fingerprints or vein verification technologies. No other measurable part of a person’s anatomy, beyond DNA, offers a more verifiable means of authentication than the living human iris – vastly superior to fingerprint, hand geometry, facial or voice recognition. Iris recognition is fast, reliable, provides certainty and remains stable throughout one’s life. In addition, iris scanning is remarkably secure, achieving “false positives” at rates as low as 1-in 1.5 million. This compares to 1-in-1,000 for fingerprint scans. The newer iris-scanning technologies use video (at 20 frames per second) to

capture the iris. This can be done almost instantly, by simply asking your customer to direct their face towards the camera for only a moment.

Now you KNOW Your Customers… and you can Know Your Employees, Too.

Once credentialed, all future transactions with the customer can be conducted on the basis of, first, authenticating the individual before allowing any activity that grants access to assets, or which requires an identity authentication in order to be in compliance. USB cameras installed at teller windows, new account desk, loan desk and safety deposit area can enable quick and easy authentication anywhere in the branch.



The extent to which the credential can be integrated and utilized across a bank's operations can be expanded in a variety of ways, as well. For example, iris scanning can fairly easily be added to ATM 's. Also, customers can voluntarily elect to require iris authentication for any online or remote banking. This is enabled through a small, mobile iris-scanning camera that can work with tablets, laptops and desktop computers.

After the biometric authentication infrastructure is available, the organization can then enable employee-credentialing to allow access to physical locations within the branch, to workstations, vault areas, safety deposit areas and whatever other access control concerns the branch might have. Additionally, the same two-step process for onboarding new customers can just as easily be applied to

onboarding new employees, thus minimizing the risk that potential "inside" accomplices working with organized crime might infiltrate your operations.

Conclusion

The days of "password and pin" security are nearly finished.

Every day brings newer, more shocking stories of the latest security breach at major institutions. Identity data is being stolen at unprecedented rates, and the criminal organizations that ultimately end-up in possession of this data are systematically attacking the financial services infrastructure.

Worse, a new brand of identity-theft criminal, armed with intricately detailed information about their intended victims, is able to present at brick and mortar locations in a manner that is practically undetectable utilizing current best-practice methods. Such criminals come to the branch bearing professionally forged ID documents, and are prepared to answer the questions posed by 3rd party databases that are used to confirm their identity. Financial institutions are left exposed to the array of possible fraud losses resulting from such infiltrations, as well as to a slew of ever-increasing penalties and litigation resulting from failure to comply with federal and state identity authentication legislation.

The shift in the "identity authentication paradigm" that needs to occur is now available through existing technologies. High level "forensic" ID document authentication, coupled with biometric credentialing of customers will allow the bank of the future to ensure that only those individuals that ought to be accessing the assets under the bank's protection are granted such access.

The savings institutions that are the earliest adaptors of this technology will be able to position themselves uniquely within the marketplace. As consumers are barraged with information about how much their personal identities are under threat, they will jump at the opportunity to find a safe-haven with a banking partner that promises to protect their money and other assets form identity thieves.