

# **New Directions for ID Authentication FTC Response P075402**

Kate Wambach  
Senior Product Manager  
EFD, eFunds Corporation

3/14/07

## Table of Contents

I. ESTABLISHING IDENTITY : UNDERSTANDING VERIFICATION PROCESSES.....	3
How identities are established.....	3
How identities are verified.....	4
Strengths/Weaknesses of Traditional Identification .....	5
Strengths/Weaknesses of Verification Tools .....	7
Information Databases.....	7
Transaction Monitoring Systems.....	12
The roles the public and private sector should have in establishing credentials .....	14
II. CONFIRMING THE ESTABLISHED IDENTITY .....	15
Reporting Weaknesses .....	22
Other Responses:.....	23
III. COMPARING VERIFICATION AND AUTHENTICATION SYSTEMS.....	24
Centralization vs. Decentralization .....	24
IV. UPCOMING CHALLENGES IN AUTHENTICATION.....	25

# I. ESTABLISHING IDENTITY: UNDERSTANDING VERIFICATION PROCESSES

## How identities are established

US citizens establish identities through two documents, social security card and birth certificate. Although there is a list of alternative documents that are accepted, none of these choices are viable since they either rely on the two documents listed above or are international forms of identification. The list below from a state DMV shows how few options US citizens have for identification:

### Birth date verification and legal presence requirements

- **US Birth Certificate**
- US Certificate or Report of Birth Abroad
- Federal Proof of Indian Blood Degree
- INS American Indian Card
- US Passport (**Note: US citizens need a birth certificate and social security card to obtain a passport**)
- US Military Identification Cards (Active or reserve duty, dependent, retired member, discharged from service, medical/religious personnel)
- Common Access Card (only if designated as Active military or Active Reserve or Active Selected Reserve)
- Certificate of Naturalization or Citizenship
- Northern Mariana Card
- INS US Citizen ID Card
- Permanent Resident Card
- Temporary Resident Identification Card
- Canadian Passport/Birth Certificate
- Non-resident Alien Canadian Border Crossing Card
- Valid foreign passport with a valid Record of Arrival/Departure (form I-94)
- Certification from California Department of Corrections or California Youth Authority
- Employment Authorization Card
- Permanent Resident Re-entry Permit
- Refugee travel document
- "Processed for I-551" stamped in a valid foreign passport
- Valid I-94 stamped "Refugee," "Parole or Parolee," "Asylee," or Section 207, Section 208, Section 209, Section 212d(2), HP or PIP
- Immigration judge's order granting asylum
- Certified court order or judgment issued from a court of competent jurisdiction.
- Valid I-94 with attached photo stamped "Processed for I-551 temporary evidence of lawful admission for permanent residence"
- Notice of Action (I-797 Approved Petition)
- Mexican Border Crossing Card with valid I-94



The only documents acceptable for SSN verification are originals of the following:

- Social Security Card (cannot be laminated)
- Medicare card (Note: Must have a social security card to obtain a Medicare card + age 65 or older)
- U.S. Armed Forces Identification Cards:
  - Active-DD 2
  - Retired-DD 2
  - Reserved-DD 2
  - Dependent-DD 173
- Military separation document-DD 214

Exception to the SSN requirement:

If you are legally present in the US, but ineligible for an SSN, you are exempt from SSN requirements. However, you must still provide an acceptable birth date/legal presence document for any DL/ID card application **OR** provide a valid SSN.

## How identities are verified

At the highest level, businesses verify consumers by examining state issued IDs.

- Consumers who are 16 or older are identified by state driver's license or state ID.
- Consumers who are under age 16 are identified through two government issued documents, a social security card and birth certificate.
- International consumers are identified through a passport.

Businesses who manage large sums of money (banks/other) take additional steps to verify consumers in order to meet regulatory compliance requirements. These additional steps include:

- Data Validation (Is the data in the right format?)
  - Does the driver's license number meet the field length requirements?
  - Is the social security number in the right format?
- Data Verification (Can this person be verified with other data sources?)
  - There are thousands of database searches that can be used, some of these databases have FCRA restrictions and others are considered public record databases. Listed below are a few examples:

Debit bureau /checking data, credit bureau data, fraud data, hot lists (bad actors list), check data, SSN validation, DL validation by state, signature verification, bad address (prison) , property and asset data, biometric data, genealogy, demographics, Internet Protocol, employment, payroll verification, real estate, automobile info, leasing data, bad bill payments, disconnected phone numbers, higher risk data, deceased records, directory assistance, cell phone databases, change of address, name change, public record data obtained via newspapers, magazines, trade journals, industry newsletters, tax and accounting, financial data, legislative records, business records, professional licenses, SOS &UCC business data, bankruptcy, judgment & liens, divorce, criminal record data

A few examples of database verification checks include:

- Does the name provided match the SSN record? Are other people using same SSN? Does the date issued match the DOB?
- How long has the address/phone been reported?
- Can the DMV/BMV verify that the driver's license number is valid?
- Does the area code match the city?
- Does this person have a history of fraud?
- Is there an id theft alert on the file?

When consumers transact with one another, trust is built in two ways:

- Consumer examines another consumer's state issued ID.
- Consumer receives a reference from trusted person.  
For example: Neighbors trade home improvement references all the time. If a trusted person provides a referral, trust is immediately established.

## Strengths/Weaknesses of Traditional Identification

The existing identification process has the following strengths:

1. Information is decentralized (by state and agency for birth certificate and SSN)
2. Consumers understand the requirements (2 forms of ID / or DL )
3. Agencies are readily available across the country

Identification processes also fail for these same three reasons.

1. Decentralized identification processes make it extremely difficult to verify the authenticity of the document(s) and information presented

50 different state IDs and hundreds of different passports make it difficult for businesses and other consumers to identify the legitimacy of the document. It is very difficult for a consumer to identify another person based on their ID. It is easy for a criminal to create and present a fake ID since they recognize that businesses find it difficult to recognize differences between State Ids. It takes sophisticated verification databases to uncover misrepresentations.

2. It is easy for fraudsters to steal two static forms of ID. Consumers even advertently give static information away to phishers.

SSN and DOB information never changes – it is static. Consumers forget user names, passwords, pass phrases and pictures since they have multiple business relationships that all have different requirements. In addition, this static information is widely available and easy to access. Its available in the mail box, displayed on your license, typed in plain text or announced verbally via the phone.

Driver's license numbers add another piece of information, but these numbers may only change every four or more years. Pictures and signatures are difficult to verify as these change and are not updated. They are also susceptible to forgery and disguise.

3. It is easy to obtain a state issued license using false information

The current process allows for a duplicate driver's licenses to be issued without the consumer's knowledge. The real consumer doesn't know that a duplicate was made. The fraudster then uses the data for credit, loans and merchandise. In almost half of the states, businesses are not allowed to verify the driver's license information. This rule protects consumers from unauthorized searches. However, it also protects criminals from being detected since an ID check could reveal multiple licenses issued at the same time (duplicate being used by fraudster and original license being used by legitimate consumer).

Improvements within the identification processes should consider the five items below:

1. **Create multiple points of compromise.** Rely on information beyond a SSN and DOB. Instead, build a matrix of identifying components that are difficult to map back together.
2. **Hide information.** Today, ID information is visible. Future identification cards should hide critical data elements that are not required. When additional screening is needed, businesses should be able to scan the card.
3. **Restrict access to the data.** Although cards can collect and store all types of data, new processes should restrict what and how the data can be recovered. The person who owns the data should be the only person who can unlock the information. The consumer should have a key to unlock relevant data and should be provided with information regarding their decision to disclose the information (i.e. – warnings for providing dynamic identifier,etc)
4. **Use dynamic information** (freshness date) – Use information that changes frequently. This prevents fraudsters from stealing the data once and using it over their lifetime.
5. **Make it convenient.** Don't make the customer supply new documents but instead use multiple things that are already used by the consumer. Gain a better understanding of what consumers have and what they find convenient (i.e. – credit card used for finding airline ticket, mobile phone, etc). Give the consumer alternatives.

## Strengths/Weaknesses of Verification Tools

### Information Databases

Information databases are a great method for verifying all the information presented on an ID. They enable businesses to verify consumers' ID information and the consumer's payment history and the ability to verify if there is a past history of fraudulent activity. These systems are fast (sub-seconds) and convenient. These systems enable businesses to make large financial decisions at the point of consumer interaction.

Information databases also have gaps. When the databases are not secured properly, they provide fraudsters with all the information they need to pass through identification and verification processes. Other information databases weaknesses include: the use of stale (old), incomplete and unverified information.

#### Out of Date Information:

Several of data sources are only updated daily or monthly, which opens a gap of opportunity for fraud. Criminals use infrequent database updates to their advantage by acting fast. Fraudsters usually commit fraud within the first three months of opening since they recognize that consumers will eventually be notified of these fictitiously created accounts. Several steps are involved before a business can share information on fraud with other businesses. First they have to experience a loss or suspicion. Next they have to investigate and confirm that it was fraud. Lastly they can report the person to the database. This process could take several months to report. Businesses often do not want to report fraud unless they are sure that they've identified the culprit. By limiting reports to confirmed fraud, lots of small repeat offenders avoid being reported into a database.

#### Incomplete Information

ID fraud affects all types of industries: banks, retailers, and phone and utility companies. Since many of the non-financial services based businesses do not contribute data to these consortium databases, the information remains incomplete. Furthermore, data that is contributed is often stale and lacks historical information. Consumers under age 18 and immigrants often do not have a financial history on file. This leaves another gap for fraudsters to use younger or foreign people's identity information. People without a credit history are known as thin files. The file of information on these consumers is thin or limited.

### Unverified Information

Data accuracy relies on strict adherence to sound operating rules. Aggregators rely on each individual contributor to verify the information. It is the only cost effective method for verifying all the information.

Criminals may also create a new or manipulated identity since information is never verified with the consumer. Manipulated identities involve a combination of real and falsified identity components that are used to create new lines of credit (cell phone, pre-paid credit card). Creditors then report the newly provided identity information to data aggregators who add the unverified information to their databases. This information is then used by other businesses for identity verification. Since the fraudster provides the matching data, they avoid detection.

The table on the following page includes a list of verification systems and their strengths and weaknesses:



**Table 1: Information Database Strength/Weakness**

Data Source	Description	Strength	Weakness
Internal Records	Database of negative history related to current or former account holders. This information is not shared with external parties.	Prevents FI from being hit twice by the same criminal	<p>Fraudsters constantly change credentials and/or modify data to avoid detection</p> <p>Only prevents one business from fraud, does not stop others from becoming victims.</p>
Shared Fraud Databases	Fraud data that has been aggregated from a single or multiple industries and incorporated into a central data repository that is shared with contributing members. The database can contain positive or negative information such as fraudulent account information.	<p>Affordable</p> <p>Centralized fraud database</p> <p>Multiple sources of verification</p> <p>Prevents crime ring activity</p> <p>Alerts other member participants to fraud</p> <p>Facilitates loss recovery</p>	<ul style="list-style-type: none"> <li>• Fails to catch identity thieves who have not formed a negative history.</li> <li>• Industry does not report fraudulent applications that are not associated with a loss</li> <li>• Reporting: Misclassify fraud as credit loss</li> <li>• Criminals hit multiple institutions at the same time</li> <li>• Dependent on members to provide data on a timely basis</li> <li>• Limited data – requires data from multiple businesses across the industry to contribute data regularly and on time</li> <li>• Businesses are afraid to share “suspicion” of fraud for fear of law suit or regulatory action for sharing data</li> <li>• False Positives when no rules exist</li> <li>• Unable to decline using hot lists unless it meets FCRA guidelines</li> </ul>
Credit	Information contained in the	Affordable	<ul style="list-style-type: none"> <li>• Credit risk does not</li> </ul>

	<p>consumer's credit history including: contact information, former addresses, demographics, employment, account and payment history, deceased record, and public record data. This information can be used to verify if the customer's application data matches the records located in the third party database or to determine if the customer has a poor credit history, indicating that they may have been a victim of fraud.</p>	<p>Multiple confirming sources of identity verification</p> <p>Verifies application data across the credit industry</p> <p>Investigative Tool</p> <p>Meets Patriot Act requirements</p>	<p>always equate to fraud risk</p> <ul style="list-style-type: none"> <li>• Fraud products have a limited capability to catch identity thieves since it relies on matching technology</li> <li>• Bureaus do not verify the data – lets identity thieves create synthetic identities</li> <li>• Stale data</li> </ul>
<p>Public Records</p>	<p>Information about a person that is publicly filed including: court filings, judgments, liens, bankruptcies, criminal records, driver's license, voter's registration, phone data, govt supplied watch lists such as OFAC</p> <p>Address and phone validation, SSN validation, DL validation, name-address and SSN data, directory assistance and telephone databases, name and address databases, change of address data, property and asset data, drivers license, <a href="#">public records</a>, <a href="#">The New York Times</a>, <a href="#">CNN</a>, <a href="#">BNA®</a>, <a href="#">CCH®</a>, <a href="#">Tax Analysts</a>, <a href="#">Bloomberg</a>, <a href="#">Dun &amp; Bradstreet</a>, <a href="#">Matthew Bender</a>, newspapers, magazines, trade journals, industry newsletters, tax and accounting, financial data, legislative records, business records, professional licenses, SOS &amp;UCC business data, bankruptcy, judgment &amp; liens, disconnected phone numbers, higher risk data, deceased records</p>	<p>Multiple sources of identity verification</p> <p>Catches fraudsters who are not using stolen identities.</p> <p>Catches criminals who do not verify if their victim has a criminal record.</p> <p>Investigative Tool</p> <p>Data meets Patriot Act compliance requirements</p>	<ul style="list-style-type: none"> <li>• Credit risk does not always equate to fraud risk</li> <li>• Fraud products have a limited capability to catch identity thieves since fraudsters already have the information that is being verified</li> <li>• Information is publicly available to the criminals</li> <li>• Unable to decline business due to public record information</li> </ul>

<p>Computer Data (Geolocation / IP)</p>	<p>Online data that is obtained from the consumer's IP address including: location (city, state, zip), domain, ISP, DMA, and use of anonymous proxies.</p>	<p>Good indicator of fraud since use of IP tracking is new and fraudsters are not aware that they are being tracked</p> <p>Investigative tool</p>	<ul style="list-style-type: none"> <li>• High False Positives</li> <li>• Unable to track AOL networks</li> <li>• As banks begin using this technology, fraudsters will evolve their techniques and will apply for accounts via the AOL network which can not be traced or will apply for the account from the same state the address is located at.</li> <li>• Anonymous Proxies – unable to determine where someone is coming from</li> <li>• Limited use – online fraud prevention</li> </ul>
<p>Consumer Supplied Data</p>	<p>Consumers supply their own data to various sources such as fraud monitoring services or magazine subscriptions. Aggregators use this information to confirm their sources and to add information to their db.</p>	<p>Method for third party to validate existing data sources</p> <p>Maintains privacy</p>	<ul style="list-style-type: none"> <li>• Data validated by consumer –lacks reliability</li> </ul>

## Transaction Monitoring Systems

Today, banks verify existing account holders by monitoring predefined activity. This monitoring is based on rules based systems. These systems may look for rules that verify the legitimacy of funds by looking for suspicious dollar thresholds or via monitoring online transaction history. Criminals are successful from avoiding detection since they know what the predefined rules are in place and they change their activity accordingly to remain under the alert threshold.

Fraudsters know that businesses do not have the ability to monitor their activity across industries or even across accounts and delivery channels within the same enterprise. They know that banks face organizational silos and have limited information and time. The more rules that are predefined, the more people are needed to monitor activity. This also creates a large number of false alerts, which cause unnecessary consumer caution.

The table below describes the effectiveness of fraud detection applications:

**Table 2: Strengths and Weaknesses of Fraud Applications**

Method	Description	Strength	Weakness
Out of Wallet Questions	<p>A series of multiple choice questions are presented to the consumer in a defined order. The questions are derived from a database of information held by a third party. Also known as Interactive Questions or Challenge Questions.</p> <p>Examples: Mortgage Payment Amount, Lender Name, Select the closest street to your home.</p>	<p>Customers have become familiar with using this type of authentication.</p> <p>Can be used across multiple channels.</p> <p>No system maintenance required</p> <p>Responses consumer provides are protected from employee access</p>	<ul style="list-style-type: none"> <li>• High False Positives – legitimate customers do not know the answers to the questions.</li> <li>• Time Consuming “customers zero out of call”</li> <li>• Does not prevent friends/family fraud</li> <li>• Subject to potential regulatory involvement since some of the questions relate to credit history</li> <li>• Medium Security– More and more companies are requesting personal information. Encourages identity thieves to obtain this information via phishing and key logging.</li> <li>• Expensive (\$.80 -\$2.00 / transaction)</li> <li>• Information is subject to theft by insiders, hackers,</li> </ul>

			<p>or data breaches</p> <ul style="list-style-type: none"> <li>• Relies on data which is subject to fraud</li> <li>• Some customers feel its an invasion of privacy</li> </ul>
Document Authentication	Business scans the document through a device. The device compares the information and ID to a set of rules and looks for inconsistencies	<p>Fast</p> <p>Eliminates room for error</p>	<ul style="list-style-type: none"> <li>• Expensive</li> <li>• Does not catch ID thieves who obtain legitimate licenses</li> <li>• Does not catch stolen IDs</li> <li>• Time consuming, slows down operational processes</li> <li>• Businesses can't afford to have a document reader for every country, state at all their checkout points</li> <li>• Device maintenance required</li> </ul>
ID Verification Rules Engines	Compares consumer information against information in a database and provides a match/no match	<p>Fast</p> <p>Affordable</p> <p>Convenient</p> <p>No software req</p>	<ul style="list-style-type: none"> <li>• Relies on complete, valid and up-to-date data</li> </ul>

## The roles the public and private sector should have in establishing credentials

The local public sector should continue to focus more attention on centralized consumer education. Currently the private sector is doing this as well.

The federal public sector should also offer consumers with services that check computers for viruses and key loggers, similar to an annual emissions test. However this test should be an optional service for consumers.

The state government should notify a consumer when a request for a duplicate license has been made similar to FACTA for credit cards.

The federal government should create a law that restricts publishing a SSN and signatures within public record documents. This only aids identity thieves. Until stolen data is made worthless, this information should be protected.

The federal government should re-examine rules that prohibit data sharing. Improved data sharing is the way that the industry will stop the use of ID theft. Criminals share data through networks and the industry knows that through improved data sharing, crime can be stopped. By using dynamic, cross industry shared data, the private sector will have the ability to detect abnormal behavior, making stolen data worthless. The re-examination of GLBA and FCRA legislation should instead consider audits for any party who holds personal identifying information such as SSN and account numbers. Current regulations scare businesses even though exceptions are in place for fraud and risk. No one wants to take a chance and share data, not even for fraud purposes without the consumer's expressed permission. Furthermore the government should work to promote a new system that does not rely on a SSN and instead relies on multi-pronged identifiers that change frequently.

The federal government should not centralize identification requirements by requiring biometrics or through the creation of new laws that require a physical identifier as this information is static and is highly likely to be the latest piece of data stolen by ID thieves as the industry evolves. Biometrics are even more difficult to replace than data or numbers. The people of the United States should have a voice and choice when it comes to their financial security within the private sector.

## II. CONFIRMING THE ESTABLISHED IDENTITY

The table below describes the identification systems that are being used, along with the strengths and weaknesses. Consumer information databases are being used within some of these solutions but not as largely as they are used within the initial customer identification process since businesses that are authenticating consumers already have a large amount of data within their own internal systems that they have not been yet able to realize. Businesses see a lot of customer activity, however they have difficulty pulling it together or have not found value since the cost to aggregate, normalize, clean and model the data could exceed the value of existing customer losses.

In customer discussions after FFIEC Internet Authentication guidance, many customers conveyed that their fraud losses were low and the software needed to become compliant exceeded their losses five fold. They also felt that these systems further inconvenienced consumers, creating confusion and increased call volumes that cost businesses additional money. There is little to no evidence that consumers are now less concerned about their financial security - they are just more inconvenienced by the new sets of questions they are requested to provide which will in the end only end up feeding the fraudsters with the information (its still static and can be given away by the consumer).

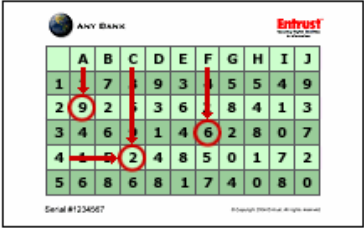
The table on the next page describes the authentication and alert systems.

**Table 3: Authentication Software Strengths/Weaknesses**

Solution	Description	Strength	Weakness
Alerts	Consumers have the option to monitor their account activity by setting up text or voice alerts via cell phone, pager, email or alt phone. Once an alert is set-up, the consumer receives a notification. Alerts can be used for balance limits, after a wire transfer is initiated, bill payment exceptions	Affordable Easy to Deploy Cost Savings - Reduce call center volume	<ul style="list-style-type: none"> <li>• Consumer becomes immune to excessive alerts.</li> <li>• Dependence upon the consumer – customer doesn’t check email – don’t know fraud occurred</li> <li>• Security issues surrounding unprotected messages</li> <li>• Fraudster already has access to account and can change alerts online</li> </ul>
Transaction Monitoring / Rules Engine	Automates manual processes that are used to detect known patterns of fraud by creating business rules that automatically detect these known patterns. Rules ensure that business processes are being followed. Rules engines access multiple data sources and may provide the following functions: <ul style="list-style-type: none"> <li>• Case Management / Workflow</li> <li>• Champion / Challenger</li> <li>• Hypothesis Testing</li> <li>• Rules Management</li> <li>• Reporting</li> </ul>	Reduces staff expenses via automation Standard policy enforcement Flexible Customizable	<ul style="list-style-type: none"> <li>• Need to update frequently to stay on top of fraud</li> <li>• Only recognizes known patterns of fraud - Need to identify known patterns of fraud before effective rules can be created.</li> <li>• False Positives – resources have to review exceptions.</li> <li>• High maintenance costs to maintain rules</li> <li>• Difficult to manage excessive rules</li> <li>• Long Implementation Time</li> <li>• Need to identify known patterns of fraud before effective rules can be created</li> </ul>
Transaction Monitoring / Neural Network	Type of model that predicts the likeliness of an event (fraud) by <ul style="list-style-type: none"> <li>- using historical data to predict future events</li> <li>- identifying behavior patterns</li> </ul>	Superior Fraud Detection Capabilities Flexible	<ul style="list-style-type: none"> <li>• Expensive (Million dollar plus set-up fees)</li> <li>• Lost opportunities if false negatives are too high</li> <li>• Relies on the quality of</li> </ul>



	<p>(typical and abnormal) using unlimited data sources</p> <ul style="list-style-type: none"> <li>- constantly building and updating user profiles</li> </ul> <p>The output of a neural network could include models/scores, decisions or profiles of consumer data.</p> <p>The effectiveness of neural networks depends on the quality and volume of data along with strong analytical expertise.</p>	<p>Customizable</p> <p>Convenient</p> <p>Invisible / Behind the Scenes</p> <p>Uniform approach across channels</p> <p>Scalable</p>	<p>data – which is subject to fraud/manipulation/incorrect data</p> <ul style="list-style-type: none"> <li>• Subject to false positives and negatives</li> </ul>
Hardware Solutions	<p>Physical devices used to verify a consumer/user. Each device is used with something the user knows such as a PIN, password, shared secret or username.</p> <ul style="list-style-type: none"> <li>• Smart Cards</li> <li>• Time and Even Synchronous Password Tokens</li> <li>• USB Token</li> </ul>	<p>Strong Security</p> <p>Effective for high risk transactions</p> <p>Proven effectiveness for internal security and commercial banking clients</p>	<ul style="list-style-type: none"> <li>• Difficult to administer</li> <li>• Expensive</li> <li>• Difficult to deploy</li> <li>• Inconvenient for Consumers (lost, stolen, damaged devices, single channel use)</li> <li>• Lacks centralized verification authority</li> <li>• Susceptible to man-in-middle attacks</li> </ul>
Software Solutions	<p>Software installed on a user's computer that is used to verify an online identity. These solutions can be compared to an electronic driver's license, where the user establishes their identity by showing the other party their electronic credential before they are given access to a system.</p> <ul style="list-style-type: none"> <li>• Client Certificate (Digital Certificate)</li> <li>• Software Smart Card</li> </ul>	<p>Strong Security</p> <p>Deployed electronically</p>	<ul style="list-style-type: none"> <li>• Difficult to administer</li> <li>• Expensive</li> <li>• Inconvenient for Consumers</li> <li>• Lacks portability</li> <li>• Moderate security – subject to key loggers</li> </ul>
Cards	<p><b>Scratch Cards</b></p> <p>Cards similar to instant lotto cards that contain a series of protected passwords. When a user logs in, they scratch off the new password in the defined</p>	<p>Affordable</p>	<ul style="list-style-type: none"> <li>• Susceptible to phishing</li> <li>• Difficult to administer</li> <li>• Inconvenient</li> </ul>

	<p>order. The passwords are stored on the bank's server and authenticated prior to use.</p> <p><b>Grid Authentication</b> Card that contains an assortment of characters that are listed in a row/column format printed on a card (similar to a bingo card). The user must complete a coordinate challenge in addition to their username and password to demonstrate that they are in possession of the appropriate card.</p> 		
<p>Phone / Voice Authentication</p>	<p>Protects access to web based resources by authenticating the user via a landline phone, mobile, or PDA. It is only recommended for important or high-risk transactions.</p> <p>To use phone authentication, the user logs into the site and enters their user name. Instead of entering their password, the mobile/landline phone rings and the user enters the secret PIN listed on the screen. This is an out of band technology that was developed in response to recent key logging and phishing attempts. The PIN changes each time the user logs in.</p>	<p>Cell phone seen as a valuable /convenient communication mechanism</p> <p>Real time notification</p>	<ul style="list-style-type: none"> <li>• Moderate Security</li> <li>• Inconvenient</li> <li>• Can only be used for high value transactions</li> <li>• Expensive (\$2.00 - \$3.00)</li> <li>• SMS messages are subject to IP network delays</li> <li>• Voice is static information and will be the next thing fraudsters steal</li> </ul>
<p>Out of Band or Phone / Voice Authentication</p>	<p>Technology used to verify an applicant's phone number or voice. This technology can be used as ancillary to compliance,</p>	<p>Links the fraudster to a phone number that may be</p>	<ul style="list-style-type: none"> <li>• Ancillary IDV Product</li> <li>• Expensive (\$1.00 - \$2.00 / Transaction)</li> </ul>

	<p>IDV and authentication solutions.</p> <p><u>Example:</u>  Branch applications: The system sends a PIN number to the registered cell phone or PDA device. The PIN number has to be verified by the user.</p> <p>Online: System calls the user's phone number. The user has to enter the PIN number that is presented on the screen.</p>	<p>traceable.</p> <p>Verifies a phone number</p>	<ul style="list-style-type: none"> <li>• Inconvenient - consumers will not find it acceptable to wait for a phone call or a PIN.</li> <li>• Subject to phone availability</li> <li>• Cumbersome user administration</li> <li>• Service problems – hackers repeatedly call phones making them unusable</li> <li>• Cell phones are susceptible to theft</li> <li>• Consumers do not want to supply their banks with their cell phone numbers</li> <li>• Static information that can be stolen</li> <li>• Does not meet needs of disabled. Fraudsters using disable phone service lines to remain untraceable</li> </ul>
Out of Wallet	<p>Challenge Questions: Rotating questions or images only known to the user and are presented during the authentication process. These products can also be used across multiple channels. Also known as shared secrets.</p>	<p>Authenticates new &amp; existing account holders</p> <p>Easy to deploy</p>	<ul style="list-style-type: none"> <li>• Expensive (\$.80- \$2.00)</li> <li>• Inconvenient for Consumers</li> <li>• Privacy Issues</li> <li>• Time Consuming</li> <li>• Moderate Security</li> </ul>
Computer Identification (Internet Fraud)	<p>There are a few companies who adopted methods to identify a user via their computer. These elements are added to behavioral profiles to prevent Internet Fraud. These include:</p> <ul style="list-style-type: none"> <li>• IP Data (Identifies Internet Location)</li> <li>• Secure Cookies</li> <li>• MAC address</li> <li>• HTTP headers</li> </ul>	<p>Detects electronic fraud</p> <p>Affordable</p> <p>Easy to deploy</p>	<ul style="list-style-type: none"> <li>• Subject to friends/family fraud</li> <li>• Moderate Security</li> <li>• High False Positives</li> <li>• Ancillary data source – ineffective as stand alone</li> <li>• Portability</li> <li>• Inconvenient for consumers – can't remember current</li> </ul>

	<ul style="list-style-type: none"> <li>• Computer time zones</li> <li>• Keystroke analysis</li> </ul>		<p>password and now they have to remember even more responses</p> <ul style="list-style-type: none"> <li>• Easy for fraudster to reissue / answer question</li> </ul>
Biometrics	Use of biometric identifier to validate and authenticate who you are: Face, Voice, Fingerprint	<p>Strong security</p> <p>Portable</p> <p>Convenient</p>	<ul style="list-style-type: none"> <li>• <u>Puts consumer in harms way</u>. Criminals highly likely to attack consumers physical security in order to obtain access their biometric vs. today where they target data</li> <li>• Invasion of Privacy</li> <li>• Difficult to Administer</li> <li>• Expensive</li> </ul>

**Table 4: Internal Processes used for Fraud Detection**

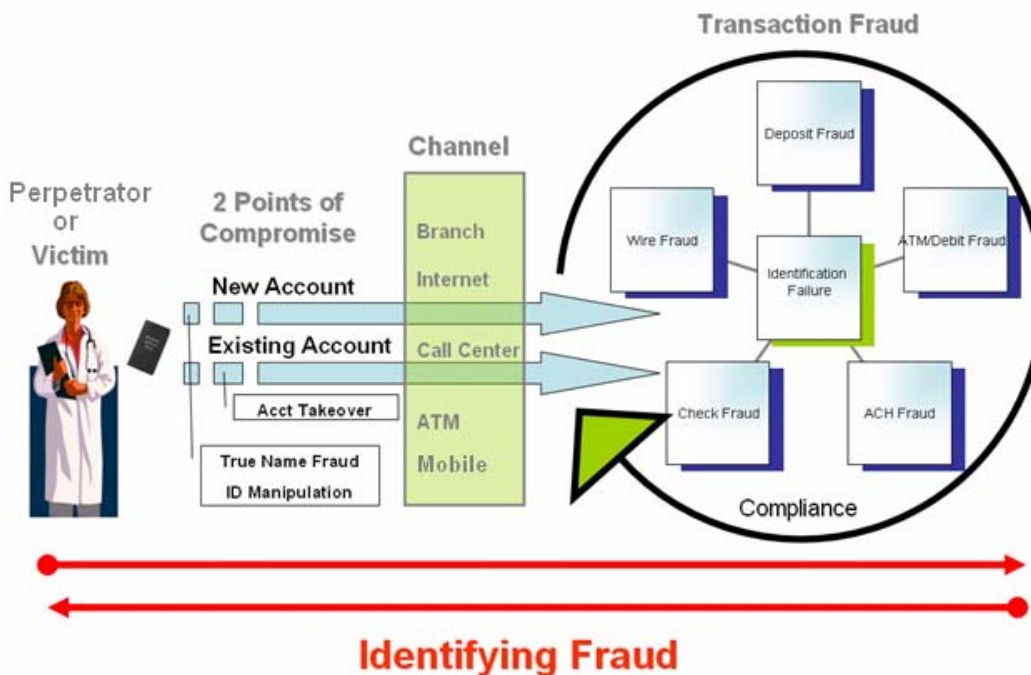
Hold Period	Monitor accounts closely for 3 to 6 months. Hold checks until they clear the system.	Fraud prevention at low cost	<ul style="list-style-type: none"> <li>• Time Consuming</li> <li>• Inconvenient for Consumer</li> </ul>
Dollar Thresholds	Hold payments that do not meet specified criteria	Low Cost	<ul style="list-style-type: none"> <li>• High False Positives</li> <li>• Resource Consuming</li> <li>• Customer Inconvenience on funds availability</li> </ul>
Manual Review	Analyst contacts the customer by phone, email, PDA or fax to verify or obtain additional information or to verify existing information.  Analyst verifies the applicants' data by cross checking disparate data sources (multiple vendors and databases).	Humans have superior detection skills	<ul style="list-style-type: none"> <li>• Time Consuming</li> <li>• Inconsistent policies are applied across accounts</li> <li>• Lacks centralized data repository</li> </ul>

## Reporting Weaknesses

The industry has a difficult time capturing the evidence related to a crime. They often mis-categorize fraud and place it into a general bucket such as check fraud. Even SAR reports contain overlapping information such check fraud and new account fraud – a newly deposited fraudulent check can also be deposited into a new account. Capturing the right evidence requires centralized reporting. Changes in reporting will consume a lot of time. To ease the burden, siloed systems should be integrated and enable centralized reporting. Centralized enterprise reporting systems will be important to improved industry reporting of all incidents.

In order to be effective, all fraud incidents should be able to be shared. Today many businesses do not feel that they can share a report of consumers who repeatedly file unauthorized transaction reports such as Reg E claims since they would have to prove who committed the fraud. Instead of being afraid to share information, the industry should feel obligated to protect one another. The industry should signal one another not to trust fraudsters who repeatedly try to scam businesses out of merchandise and money. The picture below further illustrates the pieces that should be tracked and reported:

- Who filed / committed incident?
- How long was the account opened?
- What channels were accessed within the crime?
- What types of transaction fraud were committed?



## Other Responses:

Consumer databases are not widely used when verifying existing customers since the ID information generally stays the same, unless in the case of a move, death or name changes.

In the end all systems map back to a SSN. It's the key that unlinks all the account numbers.

Data managed by the private sector has less privacy concerns than data managed by the public sector. Consumers do not seem to be concerned about privacy when their credit card purchases and online activities are monitored. Typically, a call from the bank requesting verification has had very positive results where the consumer feels that the business cares about their welfare.

However, if consumers felt the government had any access to this information, they would be furious. Consumers do not want the information centralized by the government. By keeping data managed by the private sector, the information is decentralized and protected. Database companies focus on their area of expertise (credit, debit, IP, addresses, phone numbers, etc). Consumers want the private sector to protect their business, but they do not want the government to use it for taxes or to assist in criminal investigations.

### III. COMPARING VERIFICATION AND AUTHENTICATION SYSTEMS

Verification and authentication systems provide layered security and are used for different circumstances, depending on the stage in the account lifecycle and fraud risk. Verification systems are used for lower volume, higher risk transactions where limited to no information is available, such as new account opening. These systems rely on information provided from other businesses. Authentication systems are used for high transaction volumes with limited risk such as existing account access where historical internal information can be used.

#### Centralization vs. Decentralization

The value of decentralization is reduced risk.

Example: If a criminal broke into the Arizona state DMV database and stole all the information, they would not have the Arizona consumer's bank account numbers, house key, mobile phone or credit card. The criminal won't know if they stole another criminal's information vs. a wealthy person's data. Today data breaches are such a big problem because the industry relies solely on static information that is printed on a license versus all the other credentials that make up a consumer.

Consumers are not likely to accept a centralized government identification system. It reminds them of big brother and carries high security risks, especially when the government has been involved in publicized data breaches. Instead, the government should help sponsor private projects that work with the private sector to create separate but decentralized databases that is limited for use by the private sector. Today, the private industry can not afford to create identification databases since the value and losses from inadequate identification and authentication are scattered across the world.



## IV. UPCOMING CHALLENGES IN AUTHENTICATION

Today, everyone looks at the symptoms versus the problem. The industry can win in this fight against ID theft and terrorism by taking a step back to find the root cause of the problem. Identity / data theft results when criminals use two pieces of stolen static data. I urge the industry to take a step back and instead work to **make stolen data worthless**. Making stolen data worthless will decrease the value of credit card numbers, bank account numbers and identity information by making it so difficult for the criminal to piece together the pieces of a moving puzzle that they give up. By eliminating the value of data, data breaches, phishing, pharming, key loggers, and mail theft will all be greatly reduced since there is no value in the data. In order to make stolen ID data worthless, current laws limiting data sharing need to be re-examined to allow more open rules around data sharing for fraud and risk (includes identification and authentication).