

# ACAMS<sup>®</sup>TODAY

The Magazine for Career-Minded Professionals in the Anti-Money Laundering Field

## The challenges of ID verification when accepting clients



Reprinted with permission from the December 2015–February 2016,  
Vol. 15 No. 1 issue of *ACAMS Today* magazine, a publication of the  
Association of Certified Anti-Money Laundering Specialists  
© 2015 [www.acams.org](http://www.acams.org) | [www.acamstoday.org](http://www.acamstoday.org)

**ACAMS<sup>®</sup>** | Advancing Financial  
Crime Professionals  
Worldwide<sup>®</sup>



**F**raud involving identification documents, commonly known as ID fraud, affects a growing number of individuals and organizations around the world. Worse, the interconnected nature of today's world has turned the problem into a truly global menace. Losses suffered as a result of ID fraud run into billions of dollars each year. In the U.S. alone, the annual financial losses caused by ID fraud in the corporate sector amount to tens of billions of dollars.<sup>1</sup>

Even though the financial industry is now in a much better position to tackle ID fraud than it was only a decade or so ago, fraudsters and counterfeiters are notoriously inventive, and incredibly difficult to beat. One of the areas where progress has been particularly strong is the heightening of awareness creation, as a result of which a growing number of people now understand just how important it is to protect their identity. Given the far-reaching consequences of ID fraud in terms of both financial and reputational loss, client identification has very much been in the spotlight in recent years. Banks in particular have introduced extensive measures to reinforce their client identification processes, and in doing so, have protected themselves and their clients from ID fraud.

Financial institutions now perform an ID check before accepting new clients. This process includes the verification of a client's identification document. Where such checks are not performed or conducted with insufficient diligence, the consequences can be dire—anything from money laundering to the contracting of loans or mortgages that will never be repaid.

By law, banks are required to verify the identity of every client with which they enter into a business relationship. The actual verification process is often embedded in the organization's compliance risk management discipline. However, the challenge in the customer identification process lies in the ID check itself. But how do you check an identification document? How, for that matter, would you recognize a forgery? In short, what should you look for when performing an ID check?

### Spotting a forgery

In recent years, the financial sector has launched a major offensive that targets two related objectives: fraud prevention and risk minimization. As a result, compliance risk management is here to stay. At the same time, the financial industry is constantly required to respond to legislative changes aimed at preventing and combating ID fraud and money laundering. International anti-money laundering legislation, for instance, requires customers to be identified on the basis of a thorough inspection of their identification document. In meeting these and other demands, banks have had to introduce important changes to their operational processes.

While it may seem obvious, an ID check is one of the most important aspects of the client identification process. As such, it kills three birds with a single stone: It allows attempted fraud to be spotted at an early stage, it enables banks to meet regulatory requirements and it boosts the bank's reputation as a diligent service provider. Performing the correct ID check for each transaction or interaction is therefore essential. In practice, staff often lack the knowledge, tools or confidence to establish whether an identification

document has been copied or forged. To be fair, spotting a forgery is much harder than you might think.

In 2014, Keesing Technologies conducted a survey among people across the globe who are professionally involved in the checking of identification documents on a frequent basis. The results of this survey showed that some 60 percent of those people who inspect identification documents on a regular basis are unsure about the quality of their decision. Moreover, some 40 percent of these indicated that they made little to no use of profiling techniques when linking an identification document to its holder.

### Thousands of ID documents, each with unique, individual features

According to fraud expert Daniel Suess of Keesing Technologies, "Checking an [identification] document is not as straightforward as it might seem. Even people who have received training find it difficult." The number of identification documents currently in circulation runs into the thousands. According to the U.N., some 195 countries now produce their own passports, ID cards, driving licenses and residence permits. Between them, they launch approximately 150 new identification documents each year, while retiring a great many others. Bear in mind that each of these documents is based on a unique combination of design elements and security features. Think, for example, of the machine readable zone, the RFID chip, photo protection techniques, UV and/or IR features, the watermark, the security thread or any number of security solutions such as an ImagePerf.<sup>2</sup> In practice, this diversity makes it very difficult to establish the authenticity of an identification document with sufficient certainty.

<sup>1</sup> Bureau of Justice Statistics, National Crime Victimization Survey, Identity Theft Supplement, 2012 and 2014. Identity fraud in the U.S. was estimated to be responsible for financial losses of \$24.7 billion in 2012 and \$15.4 billion by the U.S. DOJ.

<sup>2</sup> ImagePerf is a laser perforated repetition of the holder's photograph used to secure passports and ID cards.



Suess has spent many years working with financial institutions all over the world in their quest to optimize customer identification processes. According to Suess, the sheer diversity of documents currently in circulation makes it almost impossible to conduct a dependable check without the right tools or training. To illustrate his point, he explains that the U.S. alone issues many different travel documents, or passports, and hundreds of different ID cards and driving licenses, all of which are considered valid proof of ID. In addition, there are countless residence permits, work permits, refugee travel documents and the like. And that is just the U.S. You cannot expect people to be aware of, let alone recognize, the many thousands of documents currently in circulation. And to make matters worse, the quality of forgeries is improving all the time. Given the odd exception, the days when even a layman could recognize a forgery are long gone. We are often up against experienced people who use modern equipment.

### Risks

In the past, banks and other organizations have tended to keep a copy of a client's identification document on file, but unfortunately that is no longer enough. Instead, the person who previously made the photocopy will now be required to establish its authenticity. But how do you set about doing that? How do you recognize a forgery? What does the latest Canadian driving license look like? What about a passport from Mexico? And Switzerland?

It does not seem altogether reasonable or sensible to expect employees to have the answer. This being the case, they are not ideally positioned to spot—and thus minimize—ID fraud.

The most common types of ID fraud involve counterfeit, stolen or lost documents, or the use of a different photograph (photo substitution). Alternatively,

the document may be presented by someone who looks like its registered holder. This is known as look-a-like fraud. As Suess explains, a growing number of banks train their staff to recognize this type of fraud, while simultaneously providing them with inspection tools that make ID fraud easier to spot. For them, inspection with the naked eye is simply not reliable enough. On the downside, this places full responsibility for ID verification with client-facing staff. And uncertain staff may negatively affect the quality and efficiency of the customer identification process. In Suess' experience, confident, well-informed and properly equipped staff are far more likely to spot ID fraud. "Unfortunately, even trained staff who are familiar with the basic features of the most important ID documents, including the position, size and characteristics of their security features, will find it very difficult to conduct a full ID check in real time," Suess explains. Should the employee make a mistake or misjudge a document, the organization again runs a risk. And then there is the risk presented by the employees themselves. If they are distracted, or sloppy, or insufficiently familiar with prevailing legislation and regulations, the organization is again exposed to risk.

### Investing in training and tools

As explained, you cannot simply inspect an identification document. Instead, it is an art that demands diligence and precision. According to Suess, "Before every transaction, the client's identity needs to be checked and verified. The employee, therefore, plays a critical role in identification and client acceptance."

Suess adds that organizations should not assume that their employees are able to verify the authenticity of an identification document or the reliability of an identity. Moreover, any employee training program will need to reflect the type of requests received by the bank and the category of clients it services. An ID verification course will teach employees how to inspect identification documents, and how to recognize forgeries. This knowledge can then be used whenever necessary. Being more knowledgeable makes employees more confident about the decisions they make. And by applying

**Before every transaction,  
the client's identity needs  
to be checked and verified**

profiling techniques, employees are able to spot (attempts at) look-a-like fraud. In turn, this allows the financial industry to minimize the risks it takes.

In addition to training, Suess advises his clients to invest in solutions that help employees perform a reliable ID check. A well-designed and carefully implemented client identification system makes organizations, such as banks, less vulnerable to erroneous assessments and bad calls. No matter how well trained staff might be, we all make mistakes. Unfortunately some are more costly than others. Suess adds that "by minimizing the scope for uncertainty, you instantly improve security."



Moreover, according to Suess, investing in quality training programs and inspection tools makes sense across the board. Such investments not only optimize the client identification process, but also improve efficiency, security and overall risk management. People will be more inclined to enter into a business relationship with a financial institution that verifies the identity of its (prospective) counterparties. In other words, “a bank has to be considered trustworthy.”

### Practical tips

The financial sector is governed by complex legislation. At the same time, its clientele expects transparent, readily accessible financial services to be extended within a secure environment. As part of this service model, quality ID verification is a must. In response to market developments, many banks are in the process of optimizing their client identification and acceptance procedures and processes. Several international banks have already rolled out digital client identification systems and in-house training programs for their employees. For a growing number of banks, these investments are starting to pay off.

### 10 practical tips when checking identification documents

Suess has the following tips for anyone who does not yet have access to the necessary knowledge and tools:

1. Only accept secure identification documents. In other words, documents that contain security features, such as passports and ID cards. Documents that do not have security features, such as gas bills or bank statements, should never be accepted for anything other than address verification.
2. Always check the original identification document—do not accept copies, unless you intend to keep these for your own records (remember to obtain the holder's permission first).
3. Follow the same uniform inspection and verification procedure and be mindful of details.
4. Always check more than one security feature.
5. Try to perform the ID check in a well-lit area.
6. Check the person presenting the document: Carefully compare the photo on the identification document to the face of the person who presents it. Pay close attention to the shape of the eyes, ears, nose and mouth, and the distance between these facial features (they are more important than characteristics like the color or length of the person's hair).


7. Age check: Ask the person presenting the document for his or her age and compare the response with the date of birth in the identification document.
8. Check whether the document is still valid.
9. Use a magnifying glass, check for alterations, other deviations and any changes to the biographical data.
10. Check the identification document under a UV light. Genuine identification documents remain dark when exposed to UV light. Do not forget: Observing the correct UV response does not automatically mean that the document is genuine!

Do not be afraid to conduct a thorough check—make sure to take your time!

### Good investments always pay off

Prevention of ID fraud is a serious headache to a lot of banks. In meeting (international) legislation requirements and to minimize risk, banks have to enhance their client identification processes and perform an ID check before entering into a business relationship with the client. This ID check forms a significant part of the client identification process in which the employee plays a critical role. However, performing an ID check is not as easy as it may seem. Not only because of the sheer diversity of identification documents currently in circulation or the high quality of forgeries, but also because the lack of knowledge, tools or confidence make it almost impossible to conduct a dependable ID check, let alone to spot fraud.

As confident, knowledgeable and properly equipped staff are more likely to spot ID fraud, banks should train their employees and equip them with the right tools and systems to help them perform a reliable ID check. This way, banks minimize uncertainty, instantly improving security as fraud can be spotted at an early stage.

In the end, investing in quality training programs, inspection tools and a well-designed client identification system will pay off as it improves efficiency, security and overall risk management, enables banks to meet regulatory requirements and may even boost the bank's reputation. 

---

*Jacqueline van den Top, manager marketing and communications, Keesing Technologies, Amsterdam, Netherlands, [j.vandentop@keesingtechnologies.com](mailto:j.vandentop@keesingtechnologies.com)*