

public's confidence in what we do.

Your new "fake-resistant" report should carry a mixture of covert and overt security features that prevent re-creation and alteration and also allow detection of criminal activity. Other features that cause problems for the faker using standard equipment and software should also be utilised.

Let's look at these features one-by-one but first it is worth mentioning that all of the following suggestions are not rocket science and any fraudsters could easily overcome a single feature with only a modicum of skill with a word processor, image editor or OCR. But when presented en masse, they present a series of barriers to overcome and they can never be totally sure that they have identified ALL of your obstacles. Since my guess is that these crooks are inherently lazy, they will move their attention to someone else's reports that don't require so much time and effort.

Overt Security Features:

The overt features have two functions:

- To alert any would-be forger that you are aware that counterfeiting is a possibility and you are "on to them"
- They provide features that can be confirmed by the client as being definitely present or absent. This is most useful when dealing with a query over the telephone when you do not have the suspected report in front of you.

These features include highly visible elements like IRV stickers, holograms, embossed seals, watermarks and text formatting that has been clearly presented in a way to confound a potential faker.

Embossing:

Most office supply businesses can organise an embossing tool for you with a specially cut die to present your personalised information. They are very inexpensive, I think the one I have cost about £60 with the die. The deterrent for the faker is that to get one cut the same will take about 2 weeks and there will be a paper trail recording their order requirements.

Holograms:

Avoid the generic products that are freely available (usually with the words - QC-OK, CERTIFIED, APPROVED, PASSED and the like). Go for a blank hologram image that can be professionally over-printed with text and/or a logo peculiar to you. If finances allow, consider having your own hologram made with your personalisation embedded in the hologram.

Watermarking:

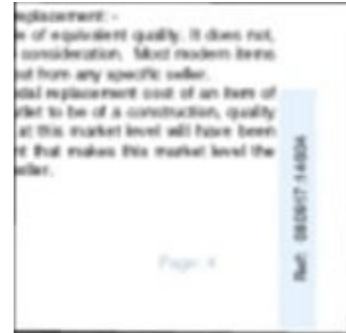
A watermark printed as you print the report is not really effective. It makes the report look untidy and is very easily reproduced. A better method is to have paper produced for you with a personalised watermark embedded in the paper.

Images of the items used in the report should be watermarked. It is amazing how often I have come across my photographs on the Internet, not always used to deceive but annoying none the less. Use a logo or cipher that you have built personally, don't use text only or generic graphics; they are too easy to reproduce. Place the watermark so it covers an unimportant part of the item in the photograph. This prevents cropping of the image to remove the watermark. Ensure the watermark is semi-transparent so it is not too intrusive and any item part it may cover is still visible. Apply the watermark to the image not to the document containing the image.

Text Formatting:

Try to incorporate some quirky text formatting somewhere on each page. Something that can be placed in the footer is ideal since it doesn't interfere with the main text and by default, will appear on every page in your report.

For example; all my reports carry a two-part reference number in text that is oriented at 90 degrees to standard text and presented against a coloured background.



Consider using some formatting that makes the text look like something else. For instance, in the two Declaration areas of my reports I have

a panel with a barcode style background and the reference number over printed using a now defunct font. It looks like it could be some sort of security feature that requires barcode reader to decode, it looks like it could be a lot of things actually. The faker will not know the significance of its presence so will not know how to handle it. It also confuses the hell out of an OCR but more on that later.

Covert Security Features:

The single function of the covert security features is to be able to positively state whether you produced the report or not, no matter how meticulously the forger has done his job. This would obviously occur after the report has been presented to you for verification.

It is important to include these features by default rather than relying on memory to incorporate them. I would suggest that these ideas are included in the base templates that you use to produce your reports. You must be able to make it so consistent that you could stand in court and swear till you are blue in the face that you did NOT produce that report

Hidden Logo/Character

Ideas for covert features include placing discreet printed marks in areas that are

not normally seen when the report is bound, for instance a very faint small logo, character or line placed at the extreme edge of the paper usually hidden by the spine (you will have to alter your print driver settings to achieve this).

Flagged Punctuation

Try using what I call "flagged punctuation". These are punctuation marks that are a very slightly different colour to the remainder of the text (e.g. dark grey versus black). Under normal scrutiny, they go un-noticed. Closer examination would reveal the difference. Using punctuation in this way has added benefits in tricking the OCR.

Ultra-violet ink

Consider marking your document somewhere consistent with ultra-violet reacting ink. The UV pens used for marking your postcode on electrical equipment will work just fine.

Every time you open a new ream of paper, draw three diagonal lines down the edge of the whole block of paper, thus taking 2 seconds to mark the whole ream. Then each sheet will have three dots of UV ink on it's edge. If you load your paper in the printer the same way each time, a UV lamp will show if any or all of the sheets in a finished report have been replaced, since the diagonal lines will be broken by the replaced sheets or totally absent if you are not the source of the paper.

Other measures to consider

Confusing the OCR

My guess is that the OCR is the most valuable tool to the counterfeiter. For those unfamiliar with the term, OCR software scans a printed document or digital file and identifies areas of text and reproduces it in the nearest available font in a selected file format (e.g. MS Word). This allows the user to now edit the text and reprint. Any areas that cannot be identified as text are returned as images placed in the same position on the newly created document.

Any steps that can be taken to confuse the OCR should be employed. For instance, the above suggestion of vertical text comes out as an image when using an OCR. Ok, they have your vertical text now but they cannot edit it and you now have a reference to trace the source of the "leak".

The obscure font reference number placed on the bar code style background serves exactly the same purpose.

The tagged punctuation also serves us well here, as an OCR will reproduce the punctuation in black, if you have the original in a dark grey. So any similar document that is produced with black flagged punctuation must have been retyped from scratch or put through an OCR.

Photocopies would probably not be used to deceive but in keeping with the legal profession it is wise to sign the original in blue ink.

PDFs

Contrary to popular opinion converting a document to PDF format is not secure. If like me, you include a PDF format report for your client's convenience, this can be a worry. An OCR can be used with a PDF document and there is now very cheap software that will convert the PDF back to an editable word processor file (eg Word).

By strategically placing a heavy watermark throughout the document after printing but prior to conversion to PDF you can reduce the effectiveness of any attempt to revert the text back to editable form. The watermark text I use is "AUTHORISED PDF COPY" placed diagonally and repeatedly across each page so the top right-hand corner lines up with the bottom left-hand corner of the preceding watermark, thus leaving no entire line of text unprotected. The watermark needs to be darker than normal but I have found a light grey fill on the text with a dark grey edge to the font elements confuses the OCR and the result is total gobbledegook.

If you include a scan of your signature in the PDF, ensure that this is done in black so it cannot be confused with a blue original signature.

CDs and DVDs

If you additionally supply a data disc with your reports, be sure to set your disc burning software to close the session after the disc has been burnt. This prevents files being added or edited at a later date.

Pre-Sale Documentation, Certificates of Authenticity etc

Up until now, we have discussed preventing and detecting a full counterfeit of a report or the alteration of an original document.

Little can be done to prevent production of a document that bears no resemblance to the genuine version. Of the two formats I have encountered, one was produced on a Microsoft Publisher template and the other was a pre-printed card certificate type document over-printed with item details, value and photograph. Both indicated that I had produced the document and contained text & images/logo from my website.

These documents would be immediately obvious to anyone in the trade as being wrong, with endless references to non-existent Diamond Grading Reports or lots of flowery, meaningless language and outrageous values. Even the public would suspect that something is "not quite right".

Internet

Needless to say, the majority of the instances of a Valuer's name being used to support a con-merchant's aims, stem from the Internet. Usually documentation, typically a Valuation for Insurance or a Certificate of Authenticity, is offered along with an inferior or fake item.

The use of online software like Google Alerts is very useful to monitor the Internet for references to your name, business or website address. Once set up with creative use of search words and terms you can immediately be notified when your search criteria appear on the web.

Should someone decide to resell an item that came with documents bearing your name they would usually refer to your name and the document to try and encourage a sale or higher bid, thus triggering a Google Alert. Similarly, if your name were under discussion (or attack) in a blog or forum, you would be instantly notified. I know all this all sounds a little paranoid but bad news travels very quickly on the Internet. A disgruntled consumer who thinks that you are somehow involved in a scam can make an awful lot of noise and if left unchecked, this viral form of defamation can ruin your reputation in certain circles in no time. You need to be sure you get to hear it first.

I have had my name used for all sorts of things, from confirming that Moissonite jewellery is diamond to providing an employment reference to someone working for an agency.

Lost time and earnings

I don't think this sort of fraud is anything like widespread but it does happen. I think I have had more than my fair share of instances, probably because I am the most northerly Independent Valuer and the bulk of the scams originate in the south of England. The assumption is obviously that I am too far away to hear about it.

Little did one fraudster know that he sold a good friend of mine a pair of "diamond" earrings and one of my private clients a "diamond" ring. This particular scam was large and ate vast swathes of my time as I tried to get to the bottom of it all, assist victims and generally dealt with related phone calls that at it's height was running at about ten a day. Oddly enough, the scam that took the least amount of my time was of the full counterfeit type. I only received one phone call – and that is very worrying. The lengths that the forger went to *exactly* reproduce my report and it's presentation, took time. He/she would never have gone to those lengths for one report. Which begs the question; where are all the others? My guess is that they have gone through the system totally un-noticed. They are now "out there" like a ticking time bomb.

Conclusion

Most of my suggestions here cost little to implement, requiring just a little imagination and some time. Specially made watermarked paper and bespoke holograms can be expensive and do add a certain polish to your reports but are by no means necessary to tighten up the security of your documents.

In the course of making your reports more secure and making them "seen" to be more secure, you will not only be protecting yourself, the industry and the public from criminal activity but also raise the apparent integrity of your business and documentation.

[From the Blog of Adrian S. Smith, FGA](#)

Quantum Leap Software Solutions

Phone: 619-265-1140

3309 Juanita Street, San Diego, CA 92105

Website Code © Copyright 2010 G-Force Services. All rights reserved.

GForceServices.com

Content © Copyright 2010 QLSS and/or respective authors. All rights reserved.