Sir / Ma'am,

During my stay in the UK, I became a victim of identity fraud. I previously shared the mechanism how this happened with the concerned authorities, and this is a follow-up; with main points which I personally consider important in detection of similar incidents and detection of a pattern:

This is a summary from the Department of Justice which I am you sure have.

http://www.cops.usdoj.gov/files/ric/Publications/e03062303.pdf

I will only explain the pattern without any personal details:

EU national gets a job in a different EU country, in this case UK. If this position is long term (several years), the person has to terminate many relationships and affairs in the country of origin - this means registered address, bank account, tax records, health and social insurance, etc; and start a new career in a different country.

Within the EU, this should be relatively easy, but for some reason it is not. This “termination of relationship with a state” can result in erasing of the concerned person from the database of inhabitants, what makes the person effectively “displaced”. As per my experience, this mainly concerns former Soviet satellites, which registers their subjects by permanent residence (registered address). This is rooted historically in tsarist Russian system which was adopted in Soviet vassals. This has very practical consequences. Unique identifier, birth number, is not used throughout Europe.

The number of EU nationals from former Soviet satellites who moved to the UK to find work after 2004 when these countries joined the EU is unknown. The fact that neither the country of origin nor the target country (an island, people usually don’t swim over the Channel to get there) have a clue how many people are moving back and forth is rather concerning. My personal opinion is that this population subgroup can easily become subject to abuse and trafficking because of their lack of family back up (result of long term family policies pursued by the Communists), failure of their home countries to recognize the threat (due to utter incompetence and profound corruption and nepotism), and reluctance of the target country to deal with the issue. For more info on human trafficking see the Blue Planet by M Bayer, NDIC; p 53 / 76 of 205. http://ni-u.edu/ni_press/pdf/The_Blue_Planet.pdf

Results of census can provide very good insight into migration and raise red flags with regards to people who are apparently or factually missing. Only in the Czech Republic, according to the results of census, there are roughly 300.000 people not accounted for in the census. This fact, that there is a large population group of young Eastern Europeans becoming victims of extremely aggressive human rights trafficking groups, is not reflected in the latest human rights report at all: http://democrats.foreignaffairs.house.gov/archives/108/92389EU.pdf

This problem does not seem to worry Czech human right professionals, because at least one of them, Martin Herzan, who worked in human rights commissions at governmental and EU level, is more concerned about writing books on Illuminati and New World Order than human rights. http://www.martin-herzan.estranky.cz/

Technical aspects of identity fraud – based on practical experience and my current understanding of the system which is incomplete:

1) Employment agency requests way too much information from a jobseeker, including a copy of passport, NI number (if not copy of NI card), copy of driving license, date of birth, any previous names, full employment record, full educational record, copies of certificates, etc. After a series of job interviews, this person provides a perfect material for identity theft.
2) According to ICO, this practice is perfectly legal. The only defense measure is reliance on the DPA 98. Some employment agencies ask applicants to tick a box where they agree to wave their rights as per DPA 98. This is rather common practice in the UK.
3) Person A gets employment in company X. Corporation X uses personal details of A in the following form:

   A1: NI number correct &name with spelling error (1 letter = typo / administrative error)

   A2: NI number with a typo (1 number = typo / administrative error) & correct name spelling.

   Person A gets dismissed and has (naturally) problem to get welfare benefits (whatever – jobseeker's allowance, housing benefit, etc). HMR&C somehow cannot get right the person's name, date of birth, address, NI number, etc, correct. From correspondence it becomes obvious that there can be more than one independently kept records for one identity at a time, apparently stored in different offices, so they cannot be easily cross-checked and matched as identical. For some reason, all variants are kept administratively.

4) For some reason (recession; changes in the industry including outsourcing and off-shoring etc; but also spreading of malicious rumors what is a favorite technique of some British agencies since the 1930's – see Defense of the Realm) the concerned person does not get a job and has to leave the country. This is done in very specific cases e.g. to get privileged access to information sources or to dispose of a witness etc.

5) Hypothetical scenario: The Corporation gets rid of A but keeps A1 and A2 on file. This makes little sense from financial point of view (no point in paying a non-existent employee) but makes perfect sense if we consider "subscription value" of such an employee. People who sign somebody else's BS are hard to come by, and it is better if they do not know about their involvement. As corporate operations are confidential stuff, an employee who physically left (person A) would never learn about the fact that he actually "stayed"!

6) OK. Person A1/A2 (original is A, that is gone) has got to obtain some ID card. I am not entirely sure how this is done, because the two people are not biologically identical, and their biometric details therefore differ. This does not matter providing the person gets new IDs in addition to his original identity (which is B), which is not used for travelling purposes, but only in places where biometric details cannot be checked. Typically in employment settings. So in such a hypothetical scenario, person B would use identity A1 / A2 to sign whatever is needed and happily carry on

living as person B. This principle is described in similar way in that DoJ document (see above). Person A would never learn about this use of his identity for a criminal activity.

7) This mechanism is totally impossible without the cooperation of insider within HMR&C, because that is the place where "cloning" of the records occurs. The employer would not be able to do this without the cooperation of HMR&C.

Red flags signaling risk of identity theft:

- Series of typos in administrative records which are difficult to correct (one typo gets corrected, another shows up immediately)
- Several people with exactly the same name and similar looks or career paths and interests (this indicates an artificially created shadow which can be confused with the original).
- Somebody else signing for the person's mail. Person A complains about undelivered post or that post does not get delivered to the addressee. This can be easily documented as most business post goes in and out as recorded signed for mail.
- Corporations with extremely high turnover of employees in key positions

Specific identifiers should be routinely used to establish the person's real identity. Voice recognition technology greatly helps if compared against a standard sample recording. All other biological identifiers, search dogs, knowledge of specific information, etc can help, too. Relying on "utility bills with name and address" as frequently used in the UK is plain scary.