A new identity theft: Not even your name is safe online

By James Whalen
Aug. 26, 2014

Every day, countless transactions occur through the Internet in which one party agrees to the terms of another through some sort of electronic substitute for a physical signature. These processes can be completed using either of two distinct methods: electronic or digital signatures. While electronic signatures are far more common, they are easily forged and create mistrust between the two parties involved in signing. Not being able to correctly attribute signatures to their signers can have devastating effects, as was demonstrated in the buildup to the 2010 Foreclosure Crisis.

Despite the disadvantages, the vast majority of businesses currently use electronic signatures in their online dealings. Though a federal law enacted in 2000 called Electronic Signatures in Global and National Commerce Act (ESIGN) seemed to give them legal authority, a second law adopted by 47 states called the Uniform Electronic Transactions Act (UETA) seemingly struck down their legitimacy by requiring that e-signatures must be attributable to the signer. What this means is that without being able to verify that the signer is in fact who they claim to be, the signature has no legitimacy. The prevalent e-signature format certainly cannot meet this requirement, but has not been challenged for that fact.

While physical signatures can be matched to their owner by a handwriting expert, electronic signatures cannot reliably offer similar third-party verification. Most electronic signatures require only a typed name or an image of a signature. But it is not at all difficult for anyone signing an electronic document to type a different name than his or her own, or to download and use an image of someone else's signature. Under this flimsy protection, someone else could sign your name on a loan, take out the money, and leave you powerless to prove that you are not responsible for paying the loan back.

However, the solution to this problem already exists. Digital signatures, a far more protected alternative to e-signatures, use digital certificates in the form of a public and a private key, which is assigned to each unique user after they have been authenticated by a third party, called a certificate authority. The certificate is attached to the user's personal information, and irrefutably links the user of the code to the signature that he or she produces. This creates a situation in which the user is unable to deny that they have signed the document, a concept called non-repudiation. The assurance provided by this incorruptible link has the power to entirely eliminate the types of contract abuse that led to the Foreclosure Crisis.

Between 2004 and 2009, an employee named Linda Green supposedly signed greater than two million documents at a mortgage company called DocX. It was discovered that she and her coworkers were signing important mortgage

documents without reading them, an epidemic known as Robo-Signing. As a result, massive numbers of foreclosures were incorrectly carried out, creating the 2010 Foreclosure Crisis. It was later discovered that there were multiple different handwriting styles among the massive pile of “Linda Green” signatures, suggesting widespread forgery. This meant that the employees that were almost solely responsible for the Foreclosure Crisis could not be held accountable for either their irresponsible signing or their illegal forgeries. The scale of the problem that resulted made it quite clear that improper signature attribution can have a massive national and even global impact. But no significant actions have been taken in the US to prevent a similar crisis from occurring again.

Unlike the United States, other technological leaders have begun to make steps towards enforcing the massive advantage of digital signatures over electronic ones. The high court of India recently ruled that only digital signatures can be recognized as legally binding, allowing Indian businesses to take part in truly trustworthy online transactions to a greater extent than anywhere else. The European Union is also in the process of creating a law with a similar goal in mind.

The United States has fallen behind in its legislative ability to provide businesses and legal systems with secure online transactions, but there are existing companies ready to step in and get the ball rolling in the right direction. Image-X Enterprises is a pioneer in this regard, providing e-signature, e-notary, and other important services with the protection of the digital signature process, using the incredibly secure NSA-developed technology described above, called public key infrastructure. Each of their various services runs on the ESignIt framework, a robust and efficient implementation of the digital signature format. In designing this product, they have created a way for real accountability in online transactions in a way that could prevent calamities like the Foreclosure Crisis from occurring again, and could lead the way towards a more secure online environment.