Maintaining Consumer Confidence in an Era of "Privacy, Lost"

October 17, 2017

The massive Equifax loss of 143 million non-consenting individual's information in the US, Canada and UK presents more challenges for customer protection. Detailed financial data and private identifiers were included in the incident stemming from fundamental patch management latency. This consumer information loss aggravates an already challenged digital society seeking mobility-based services. Digital enterprises strive to provide those services across channels including social, mobile, email and web. Being able to proof their own consumers ubiquitously is a critical function for those enterprises. Unfortunately, attacks on proofing information and providers such as Equifax are to be expected given the value of that information in the wrong hands. Equifax will likely suffer reputational harm and consumers whose privacy was compromised will be potential fraud victims over an extended period. There is not a clear path for consumer reparation – credit monitoring, cancelled credit cards deal with the issue tactically.

Organizations that aggregate identity information or provide identity as a service are simply a natural target. While focus has been on the nature of this specific breach and a failure in patch management, the persistence of attacker motivated by financial crime guarantees simple hygiene won't stop the problem, perhaps slow it at best. In this case the target data included full names, social security numbers, dates of birth, home addresses, and other financial and personal information. Our personal data is "out of the bag" given this recent event in addition to earlier breaches of PII including the US Federal OPM agency. Criminals can package and sell our complete 360 identity on the dark web.

Many smaller financial services and other firms may be overly reliant on traditional question-based identity proofing, which have been an ongoing practice for years. However, fraudsters have a larger treasure trove of detailed information they can use to undermine those controls at regional banks, mid-tier 401K providers, or online providers of credit. Some larger firms have been working this issue by incorporating alternative methods to enhance question-based proofing. There are emerging ecosystems, guidelines, technologies and methods that eventually will fix this situation but in the meantime individual consumers will bear the brunt of policing their accounts and credit facilities.

We know this type of attack on personal information will happen again and again. Our basic approaches to building systems and transactional models must incorporate safeguards to guard the identity integrity of the millions of people affected by this breach. Why are enterprise architects not building around new capabilities that support internal, B2B, B2B2C transactions that support consumer transactions but in a privacy enhancing manner? Can we design a privacy fabric that includes identification services, trustworthy federation and repairable de-identification?

Your organization's approach for consumer identity management needs to be robust and diversified to overcome broad reaching privacy loss and maintain consumer confidence. Re-designing your identification services as a services bus can support resilience and identity source diversification. Risk-based approaches that also leverage privacy techniques must shape your identity assurance standards and technology selection.

As more stolen consumer information is available, account take-over fraud has increased and the attackers have become more brazen in their exploits. This in turn forces targeted organizations to increase assurance levels in identification processes. But this is directly opposed to the consumer desire for frictionless mobility.

Those very same consumers are becoming more educated on the need for protection. Companies with the best consumer experience win and the modern-day consumer expects mobility and protection together.

Why haven't we built this yet? It's not a technology problem….

A new paradigm for online security and privacy demands governance, new transactional patterns on top of distributed technology. The recent NIST 800-63 revision 3 updates are timely and helpful for consumer IAM practitioners but they cannot completely define your program. Even smaller organizations can stand to gain from the most basic NIST update stipulating separate measures for quality of identification, authentication and federation. The solutions to those three distinct capabilities are different and cooperate to provide overall on-line assurance.

Supporting your digital strategy for consumer journeys and factoring in key areas of federation governance must also be considered. For instance, it makes no sense to invest in identification and authentication for your portal if you allow a social network to front end your consumer experience with lower assurance.

Care in the handling and avoidance of storing personal information are required for on-line transactions in the digital, consumer centered age. As an example, the unencrypted storage of elements used to reset a password make it too easy for attackers who have gained a foothold in your directory to accomplish broad account takeovers.

We need to "build security in" but we must build privacy into that security

Be it the European GDPR or the US FIPPS Privacy frameworks, there are important touchpoints in your privacy and security programs. How do you Proof and Protect simultaneously? If you do not reassess your proofing mechanisms now you could have consumer breach, fraud, and privacy matters lurking despite significant expenditures in multi factor, second factor, continuous authentication, and monitoring.

Every time you consider security you must also check privacy. Think about how you are distributing information across your global high speed directory supporting your consumer log-ins. Should this be zoned by privacy regulations? Perhaps an encryption approach with in-country key management will suffice? Are there tokenization approaches to record proof of identification vs the answer to the proofing. A government issued id sitting in a globally replicated non-encrypted attribute is not acceptable. Some organizations require broad access entitlements to directory searches in support of their transactional needs.

It's the ecosystem

Let's be clear, the solution cannot be implemented by your organization alone. We need a federated fraud network, a new transactional ecosystem. With a secure privacy enhancing foundation tied to a governed transactional model with immutable identifiers. Your solutions and strategy need to be focused on the following evolving areas of innovation:

What you know isn't enough. What you are *alone* solves authentication but not proofing. What you have needs to be introduced in any case. And they need to work together, privately. The final solution needs to be thoroughly assessed for attack weaknesses using threat modeling and software testing.

-The TUV/OpenSky Consumer Identity Center of Excellence
For more information, contact OpenSky at info@openskycorp.com.