BitMint Technology

NΦΦANCE

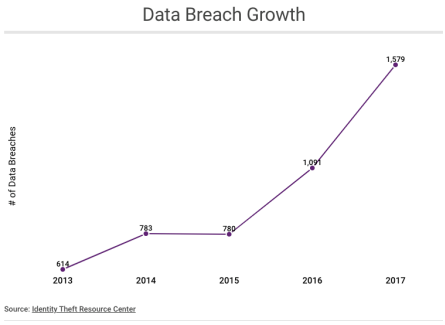
Entraping and Repelling Identity Thieves

NOOANCE: US Patent 10/395,053

De-Victimizing Identity Theft Victims

Stakeholders Roll Call

Walls crack, fences fall, and personal financial data is compromised time and again. 158 million social security numbers were exposed in 2017, 31% of them are likely to experience identity theft, and there is no end in sight. With the help of corrupt or unwittingly insiders, hackers harvest the identity credentials of the public. It is time to turn the tables on the fraudsters. We do so through a fresh idea: make it unprofitable for the hacker to hack your data. Then they simply will go elsewhere. This is done by creating a nuance between the data kept in the individual phone, and the data stored in the merchant's, bank's or government's database. When an identity thief is trying to steal an identity using the stolen server's nuance, the server (i) realizes that this is a fraud, and (ii) that the server has been compromised. The power of this Nooance^{TM} technology is in establishing a subtle nuance in the way data is written. It's not encryption, the data is absolutely readable, but it is nuanced -- and the thief cannot mark off the marker that paints him for what he is: a data thief. Identity thieves will not buy nuanced data, and then hackers will not bother stealing it. So merchant, bank, government -- keep all your walls and fences intact, but find reassurance in the fact that hackers will not challenge them because your nuanced data is worthless for their purpose.



Any merchant, bank, or government office implementing Nooance will also guard its customers and users from identity thieves who stole identities long before the Nooance is implemented.

* * *

This document is an introduction to the Nooance Technology and its prospective implementation. It is designed to identify potential stakeholders that will come together to establish the business initiative that would bring this technology to the market.

Introduction: A typical American citizen has its personal identity data stored in countless servers operated by banks, shops, corporations and government offices. Each of these databases is vulnerable to hackers. And when a database is compromised, a large number of people are violated and their private information is stolen, and subsequently abused through identity theft.

Identity theft is the most serious problem on cyber space. It is the bone of contention between hackers and defenders. The score is not encouraging. The most sophisticated banks, merchants and corporations, even the NSA have been hacked. Business as usual is not a good strategy. Fresh thinking is called for.

Enter Nooance:

Nooance is the name given to a new technology that calls for establishing a nuance between the private data written in the owner's phone or device and the same data as it is being written on the server's database.

Nooance is not a cipher, the data is not encrypted. It is plainly readable both on the phone and on the server. It is nuanced, that means the data is distinguishly marked. When a thief gets a hold of the server's version of the data he is blind to the nuance difference between it and what the phone of the owner of the data holds. When the thief uses the stolen credentials to masquerade as his victim, the server immediately realizes that the log-in is done with stolen data, so the fraudster is denied access, and moreover, the server realizes that it had been hacked.

The next thing that happens is that the server is re-loaded with a newly marked nuanced data, which then denies the sophisticated hacker from re-nuancing the stolen data to succeed in the fraud.

The arch hackers who are smart enough to overcome the cyber defense of banks and large merchants, harvest the personal data wholesale, and then sell them to identity thieves. When the Nooance technology catches the identity thieves and denies them their prey, they stop buying this entrapment data, and when the master hackers can't sell their ware, they make sure they hack only servers that don't use Nooance.

That is how the Nooance protects its deployer. Nooance works on top and in addition to any wall or fence your data is hiding under. It kicks in when these walls and fences have been compromised (as they so often do), and it renders the deployer of the technology to an unattractive attack target.

This basic deployment in one store or bank is applicable only for that store or bank. Since the stolen data is not encrypted, the thief can use it to steal identities elsewhere.

Now think about it: one big bank, or one big department store, deploys Nooance and thereby protects its customers from being victimized by anyone breaching the server of that merchant or bank, but other merchants or banks are still vulnerable.

Unless -- they rush to deploy Nooance too.

In other words, the initial success of Nooance gives rise to a strong viral spread with very impressive business implications. Which is why Nooance is a highly attractive proposition to stakeholders blessed with vision and foresight, and jumping in on the ground floor.

We are at the stage where the technology has been specified, recognized as novel, pioneering; a respective patent issued (US patent 10395053), and the patent holder (BitMint) is exploring the best implementation route. And for that, BitMint is now running a roll call, enlisting entities interested in further study, review and consideration of the Nooance option.

Operational Features: Nooance technology is backroom deployment. The user and the merchant's people will not be procedurally burdened, will need not to learn a new operation, nor change any habit. Software is being installed both on the customer's phone and on the managing server, with no hardware implementations, nor add-ons.

Nooance technology does not replace, nor diminish any cyber security defense in place. It does not create any recognized new vulnerabilities. It prevents future identity theft, as well as it helps past victims of identity theft.

Helping Out Identity Theft Victims today: An ever larger number of Americans suffers from inexorable identity theft. While payment cards may be readily replaced, social security numbers and date of birth are a lock in, and a biometric data is forever. Today these victims are violated time and again. When Nooance comes through these victims would be victims no more. They would be given the nuanced version of their private data, which the identity thief would not have. And unlike the raw private data, the nuanced data is replaceable. An individual who was personally violated will be given a new nuanced version and will shut the thief out.

Prospective Implementation Route: The initial list of potential ground floor players will be consolidated to the bonding few who will then cooperatively chart the implementation path ahead.

At this stage, one can only outline a possible implementation path as a first draft, here it is:

1. Sending the word out regarding this opportunity (this roll call document)
2. Building a communication platform for the roll call group
3. Conducting a technology review with technology people from all stakeholders
4. Specifying minimum viable products to showcase the technology
5. Establishing legal ground for the enterprising entity
6. Raising development and deployment money
7. Assembling a development team
8. Identifying the first deployment target
9. Development
10. Deployment
11. Showcasing Operation
12. Evaluation
13. Post Evaluation Steps

The Role of BitMint: BitMint builds itself as a technology hub, exploiting the new horizons illuminated by quantum randomness. BitMint aggressively develops cyber security and digital currency technology, and is currently logging more than 40 patent applications, about a quarter has already been granted or allowed. We wish to stay focused on advancing our technology, and therefore we seek an implementation partner to meet the challenge of bringing BitMint technology to market. While BitMint initiates this roll call, as things develop, we are perfectly comfortable in taking a back seat, focusing on technology support, inviting a good leader to bring the IP to the market.

Stakeholders Categories: This roll call should be regarded as a broad based invitation to all relevant categories of stakeholders. Such are: (i) merchants, banks, corporations, government departments that would benefit from deployment of Nooance, (ii) organizations dedicated to help past victims of identity theft, as well as organizations aiming to prevent future violation of private financial data, (iii) cyber security providers, (iv) payment technology providers, (v) market consultants, (v) academics, and (vi) state and federal government entities.

Notes: The subject technology of this roll call is specified in the public domain in the form of US Patent #10395053. Additional IP is in the pipeline. The technology utilizes the emerging cyber resource of quantum randomness. For a background read, please refer to the following article published by the World Economic Forum in Davos Switzerland: "What a 100-year-old idea can teach us about cybersecurity" https://www.weforum.org/agenda/2017/11/what-a-100-year-old-idea-can-teach-us-about-cybersecurity

The roll call is coordinated by Ms. Dolores Perillan, Strategic Planner,
Dolores@BitMint.com and
Gideon Samid, Chief Technology Officer, Gideon@BitMint.com 571 214 9814