Digital Banking & Legal Identities

Guy Huntington

Huntington Ventures Ltd.

March 9, 2021

Current Pain Points For Customers & Banks:

- Banks customers and revenue bases slipping away to new fintechs and tech giants
- Customers concerned about privacy cyber security ID theft financial loss
- Weak legal identity across different countries
- Banks pay for identity fraud
- Ad fraud is about 1 in 3 clicks

Solve Problems of Billions of Dollars

- The planet is full of crappy legal identities, i.e. there's LOTS OF FRAUD
- **Companies pay the price for this**. e.g. "Costs of a Crappy Legal Identity"
  - https://www.linkedin.com/pulse/costs-crappy-legal-identity-guy-huntington?trk=portfolio_article-card_title
- **Customers also pay the price for this**, e.g. "Synthetic Identity Fraud – 1 Million Kids a Year"
  - https://www.linkedin.com/pulse/synthetic-identity-fraud-1-million-kids-year-guy-huntington?trk=portfolio_article-card_title
- **Advertisers pay a price for this**, e.g. $42 billion a year!
  - https://www.linkedin.com/pulse/advertising-fraud-identity-future-guy-huntington?trk=portfolio_article-card_title

Requirements For Thinking Outside the Box

- Must allow a customer to control their own legal identity and use it anyplace, anytime, to various degrees, physically or digitally, within each country and the planet
- Must be able to verify a customer's identity across all different banks' identity systems, while at the same time maintaining each bank's privacy over their relationship with existing customers
- Must work from infants on up
- Must also be able to address complex legal identity relationships, e.g. parent/child, child/legal guardian, power of attorney etc.

Requirements For Thinking Outside the Box

- Must be easy to use, i.e. leverage different types of biometrics, and also potentially use biometric wristbands for kids et al, which can be linked to cell phones
- Must allow for rapid identity verification and authentication, to varying degrees of assurance based on transaction risk
- Must address:
  - Weakness of biometrics – what happens when someone steals customer's biometrics, i.e. they only have one set?
  - Potential successful hacks of bank's legal identity stores with criminals gaining access to customer biometrics

Requirements For Thinking Outside the Box

- Creates a closer relationship between the bank and customer
- Creates new revenue streams
- Ability to address identities from these types of emerging markets:
  - https://www.forbes.com/sites/cathyhackl/2021/01/29/how-brands-can-thrive-in-the-direct-to-avatar-economy/?ss=cmo-network&sh=3f675837417c
- Be able to rapidly change due to the pace of technological innovation depicted by this curve
  - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf

Requirements For Thinking Outside the Box

- Anonymize payment system, being able to prove what you need to, when you need to

Solution Framework:

- Bank has trust - Leverage It!
- Biometric basis for trusted financial intermediary (better than Google or Apple) across all platforms
- Banks issue ID’s for family members from infants up
- Leverage biometrics on customer phones
- Leverage biometric customer wristbands for infants/kids
- Build universal ID and payment platform
- Anonymize payments, and even web, but prove what you need to when you need to

Solution Framework:

- Don’t store customer’s actual biometrics in bank systems, but still use them to verify customer identities
- Issue customers anonymous biometrics for fingerprints, iris, face, voice and DNA - then use these based on risk
- Customers use bank issued AI leveraged personal identity access management (PIAM) system to manage their identity, data and consent
- Create an identity registration system for customers’ emerging smart digital identities, which can work anywhere on the planet

Solution Framework – Create New Revenue Streams:

- Create new revenue streams for banks by charging advertisers increasing amounts for release by customer's of their identity information the bank attests to
- Create new revenue streams by charging other enterprises increasing amounts to verify a customer's identity
- Create new revenue streams by allowing customer's smart digital entities to purchase goods/services on behalf of the physical customer

Solution Framework:

- Create a global, bank interop, banking identity verification service which:
  - Protects each bank's privacy
  - Allows for anonymous queries from each bank about a customer's identity to verify them
  - Maintains global bank standards and 24x7x365 security for interop customer identity legal identity, API to access files, and customer personal identity access management (PIAM) systems

At the Heart of the Framework…

- At the heart of the solution framework is Toda, PIAM, API, biometrics, and the banking interop
- The next slides discuss this in greater detail..

Toda

- “Toda – A Brief Introduction” https://engineering.todaq.net/toda_brief_intro.pdf
- “Toda Primer” to understand how Toda works https://engineering.todaq.net/TODA_Tech_Primer_v1.0.pdf
- “Toda Proof Structure” https://engineering.todaq.net/todapop.pdf
- “TodaQ API” https://docs.developer.todaqfinance.net/
- Toda Technical Documentation https://engineering.todaq.net/
- Your and you team also might be interested in these three blogs written by Ben Goertzel, Toufi and Dann:
  - https://blog.singularitynet.io/the-todalarity-is-here-part-one-singularitynet-toda-synergy-at-the-core-b1b84d07065c
  - https://blog.singularitynet.io/the-todalarity-is-here-part-two-the-rapidly-expanding-toda-sovtech-ecosystem-c0c225ac7d37
  - https://blog.singularitynet.io/the-todalarity-is-here-part-three-a-product-accelerator-for-driving-the-decentralized-ai-b1e60b13cc5c
- A Toda IP protocol is under development
- I’m working very closely with Toufi Saliba and Dann Toliver, co-author of Toda
- Toufi is also global chair, IEEE AI Standards, who I’m also working with regarding creating AI system legal identities

PIAM, API

- I strongly suggest you first read this paper, “Secure, Network Based, Legal Self-Sovereign Identity”
  - https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf
- In particular, regarding PIAM read pages 31-33
- Re the API
  - Look at page 6, a high level architectural model
  - Read pages 29-30

Why PIAM is the Key…

- It will become a customer's "AI assistant" advising them on who to release their legal identity, biometric & behavioral data to, as well as…
- Creating contracts, on the fly, between the customer and third parties, as well as…
- Acting as the decision advisor on things like retail purchases, financial investments, relationships, et al
- **THUS IT BECOMES VERY CLOSE TO THE CUSTOMER**

Customer Relationships…

- I'm an old guy, who's created many identity architectures for large enterprises. My view – WHAT WORKED IN THE PAST ISN'T GOING TO WORK IN THE FUTURE
- So, once I had an understanding of Toda, LSSI, BCLSSI et al, I then sat down and wrote out how it would all work for an enterprise as a series of LinkedIn posts:
  - "Rethinking Enterprise Identity" - https://www.linkedin.com/pulse/rethinking-enterprise-identity-part-vii-summary-guy-huntington?trk=portfolio_article-card_title
- One of them was about customers…

Toda Customer Capabilities Files…

- In “Rethinking Customer Identities Leveraging Toda” (https://www.linkedin.com/pulse/part-v-rethinking-customer-identities-leveraging-toda-huntington?trk=portfolio_article-card_title) I discuss Jane Doe and her child
- As the child grows older, Jane might want to grant increasing abilities to her child, e.g. larger purchases, finance decisions, etc.
- The power of Toda is it allows Jane to create in effect a variety of different “authorization rights” which she can delegate to her child through the bank issued Toda file
- Thus, the bank issued PIAM for the child, can now quickly adapt to the new authorization rights with say retailers and the bank itself
- This offers finely detailed customer experiences

Biometrics…

- Good news:
  - They're very easy to use by the customer to identify themselves, which banks leverage to do identity verification and authentication
  - Doing so is fast and becoming relatively low cost
- Bad news:
  - We only have one set – what happens when criminals maliciously obtain them?
  - The number of data stores around the planet containing biometrics is soaring, i.e. they'll be hacked and biometrics obtained
  - Criminals with deep pockets will obtain them and do various forms of replay attacks
  - This curve means the ability to successfully attack will increase
    - https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf
- So, I'm not in the biometric vendors' camps, believing it's the be all and end all
- What's the solution?

Biometrics…Leverage Anonymous Ones

- Leverage anonymous biometrics for customer carried identification
  - Read Rud Bolle's draft 2015 paper
    - https://hvl.net/pdf/BolleAnonymousBiometricIdentifiersRevisited2015.pdf
- My strategy is to rapidly prove this out and if it works, adopt it by use of banks/retailers planet wide

Biometrics…Don’t Store Them Within Banks

- For identity verification, my strategy is to adopt the following within banks:
  - Standardized biometric registration procedures
    - Over time automate this to ensure best, standardized registration with high accuracy
  - Adopt a biometric template which digitizes each type of biometric
  - Then apply a standardized algorithm to anonymize them
    - E.g. producing a value of say XYZ
  - Discard the actual biometric, and only store the value, e.g. XYZ

Biometrics…Search on XYZ

- Banks can thus search within their databases for XYZ to biometrically confirm an identity
- Thus, if the database is breached, criminals only can obtain XYZ and not the actual biometric
- This then leads to the banking interop…

Banking Interop…

- Here's Guy's view of the planet…
- Our existing legal identity is crappy. Thus in the end, it requires jurisdictions to rethink their legal identity framework, e.g. CRVS, et al . **This isn't going to happen anytime soon**
- Thus, banks can step in. Yet, there's a challenge…
- Criminals can easily move around the planet creating LOTS of fake identities, opening up bank accounts and using credit cards et al to bilk retailers and governments
- So, from a retailer's/advertiser's perspective, they want to reduce their fraud costs, which in turn means having a high trust that Jane Doe is really who she claims to be

Banking Interop…

- Which means the identity must be globally verified
- **Which in turn means the banks will have to be able to verify an identity amongst themselves, i.e. not trusting the existing crappy legal identities from jurisdictions**
- This poses a problem for banks, i.e. they don't want to piss off their customer base by requiring them to provide biometric identities to then be cross-searched around the planet, nor do they want to release their customer's identities to others
- So, how can this be done?

Banking Interop…

- First of all, offer it as an optional service to each bank's customer base, i.e. voluntary participation to leverage PIAM BCLSSI services
- Never release the actual customer's identity, e.g. their biometrics, legal name et al, without the customer's permission
- Anonymously send biometrics to be searched by a global banking interop service, i.e. Newco

Banking Interop…

- Bank “A” would send the request to Newco using a anonymous identifier of 12345
- Newco then takes the request and sends it to Bank “B” as an anonymous identifier of ABCDE and to Bank ”C” as LMNOP
- Thus each bank has no knowledge of who’s doing the identity search
- Newco only know the yes/no match type response

Banking Interop -Send XYZ, Not Actual Biometric

- Each bank sends the biometrics anonymized as described earlier, e.g. XYZ to the banking interop service, i.e. newco.
- Each bank will search on the anonymized biometric, e.g. XYZ

Banking Interop…Match Yes/No

- If there's no match to XYZ then the bank can proceed with issuing the customer their BCLSSI and PIAM
- If there's a match, then the bank would send customer legal identity numbers, e.g. birth certificate numbers, driver's license numbers, etc. to the interop
- The interop then passes this to the matching bank
- If the match is successful, the bank and retailers, now have a higher degree of confidence Jane Doe is who she claims to be
- If the result is "no match", then the bank informs the customer, steps away from issuing them a PIAM et al, and the customer can deal with it through their local law authorities
  - **i.e. Banks should legally stay out of it**

Banking Interop – Rapid Rate of Change

- Then, there's this curve to address https://hvl.net/pdf/PatScannellHockeyStickShapedCurve.pdf
- **My underlying premise regarding legal identity is continually defending against this regarding LSSI, BCLSSI, API, biometrics, PIAM et al requires VERY SIGNIFICANT resources most banks don't have**
- Thus, the banking interop is the place to do this
- It's a commercial version of the global non-profit on page 6 of this paper https://hvl.net/pdf/SecureNetworkBasedLSSIPaperDec62020.pdf
- Based on the continual threat analysis, all banks, plus their customers/retailers, will respond in kind based on the threat level
- This is how to keep bank customer identity services secure, day after day, month after month, and year after year
- This is a concept I developed with Michael Kleeman, co-founder of many different telcos around the planet and ex-CTO of Boston Consulting Group

Banking Interop – BCLSSI, API, PIAM

- The “guts” of the BCLSSI, API and PIAM would all be to banking standards
- Thus, as new attack vectors rapidly emerge, Newco would alert banks, retailers and customers and they’d update their devices and interfaces
- Banks could “customize” their PIAM interfaces with their customer by changing the UI/UX interfaces BUT NOT CHANGING THE GUTS
- This allows individual banks to innovate, while ensuring the PIAM is still secure globally

It’s Out of the Box Thinking…

- The BCLSSI would be designed to allow for integration with jurisdictional issued LSSI if and when they appear
- PIAMS give banks the ability to reduce the increasing tech giants and new fintech’s relationship with their customers, instead increasing existing bank customer relationships
- It creates new revenue streams for their customers, while at the same time creating a flexible framework to address new emerging types of smart digital identities

It’s Out of the Box Thinking…

- I have some ideas on taking all the above and anonymizing transactions
- Which I’ll share after signing NDA’s

Which is Why I'm On Your Electronic Doorstep…

- I'm looking for what I call in my head, "The Keeners", i.e. people, banks, investors who agree with the strategy, and are keen to work on creating it
- However, as a person who's led and rescued many leading edge type projects, I fully realize the implications of deploying "new stuff"
- It requires very careful, tightly scoped, POCs, in parallel, to see what works and , more importantly, what doesn't work. Then redo until we're sure it all works as advertised. Then deploy into small pilots and once we're sure it works in real life, then rapidly scale
- I'm hoping you're one of them

Contact Information…

Guy Huntington
President
Huntington Ventures Ltd.
Cell: 1-780-289-2776 (I live in West Vancouver, BC, Canada)
Email: guy@hvl.net
LinkedIn: https://ca.linkedin.com/in/ghuntington