STAR CANADA

A TECHWELL EVENT

W12

Internet of Things
Wednesday, October 17th, 2018 1:30 PM

Combatting Threats to Payment Processing in the Era of Connected Ecosystems

Presented by:

Elizabeth Koumpan

Brought to you by:

350 Corporate Way, Suite 400, Orange Park, FL 32073
888-268-8770 · 904-278-0524 - info@techwell.com - http://www.starwest.techwell.com/

Elizabeth Koumpan

Elizabeth Koumpan is a cognitive and data leader with IBM Global Markets, with a focus on solving business problems in information architecture, analytics, information integration, and governance and ensuring we use data responsibly. She has been performing evaluation and analysis of the current technical environments and completed assessments against the set of leading practices within different organizations. She has developed reference architecture that addresses key integration, migration, and consolidation decisions and is recognized for her expertise in the area of unstructured data and her ability to understand information patterns. Elizabeth led IBM ILG Software's social campaign to develop industry white papers about information governance in the era of big data. She is a member of the IBM Academy of Technology and has led multiple studies and been a speaker at several internal and external conferences.

Combatting Threats to Payment Processing in the Era of Connected Ecosystems

Elizabeth Koumpan, Cognitive and Data Leader, IBM Academy of Technology – Member, ekoumpan@ca.ibm.com, IBM

Abstract

Changes in digital technology, consumer expectations, and social media are influencing consumer shopping decisions and altering the way people are making payments. With the extensive use of smartphones, mobile banking and wearables providing convenient ways to make purchases quickly, services in the future will be further enhanced with AR(augmented reality) to provide a superior customer shopping experience.

Consumer demands for personalized experiences, regulatory and industry initiatives forcing innovation, openness and collaboration in the payment industry, development of new models and digital ecosystems with cross – border payments transformed by using block chain technology are disruptive and accelerating change in payment processing. This new world will introduce new risks related to cyber security and data privacy. The amount of data expected to pass through and to be stored across multiple devices, systems, merchants, controllers and processors, will grow exponentially.

As the Internet of Things and other emerging technologies continue to develop, it will be important for merchants to ensure that while they introduce new sales channels, they need to address fraud and payment vulnerabilities. New standards around how the data is captured, managed, processed, protected and destroyed, will need to outline policies of data ownership, access, protection and liability.

These demands are only the tip of the iceberg for privacy, data breach notifications, data subject rights, and other requirements that needs to be met when GDPR comes into force in May 2018.

Disruptive Forces are shaping the Industry

Collaborative Payments Ecosystems

- Regulatory and industry initiatives, customer demands for personalized services, new technology are leading to increasing openness and collaboration in the payments industry.
- Evolving customer expectations and open APIs influenced industry to enable collaborative approach for services and operations.

Payments Players are shifting

- An increasing demand for customized offerings, agile solutions, and secure payments from the customers, and emerging technologies, such as AI and Blockchain, are pushing further to modernize the payments infrastructure.
- Digital payments and e-commerce are increasing competition and forcing payments services vendors to consolidate to capitalize on economies of scale.

Cyber Security and Data Privacy – investing in advanced technologies to fight fraud and data breaches

- Cyber threats and frauds are on a rise with increased adoption of mobile payments and wearable devices.
- Increased data availability, faster processing systems, machine learning technologies are pushing for RPA(robotic process automation) to adopt efficient and secure processes.
- Regulators bringing in new cybersecurity regulations , standards and data privacy protection rules.

Next Generation Payments

- Banks are witnessing a demand from retail customers for instant payments.
- Alternate payment channels, such as contactless and wearables could soon become mainstream.
- Distributed ledger technology transform cross-border payments.
- Quantum computing pose a danger to how cryptography secures information .

Emerging Payments Ecosystems

Frictionless commerce - as the world becomes more connected, technology is becoming central to the retail experience with payments to be taken as fast and easy as possible.

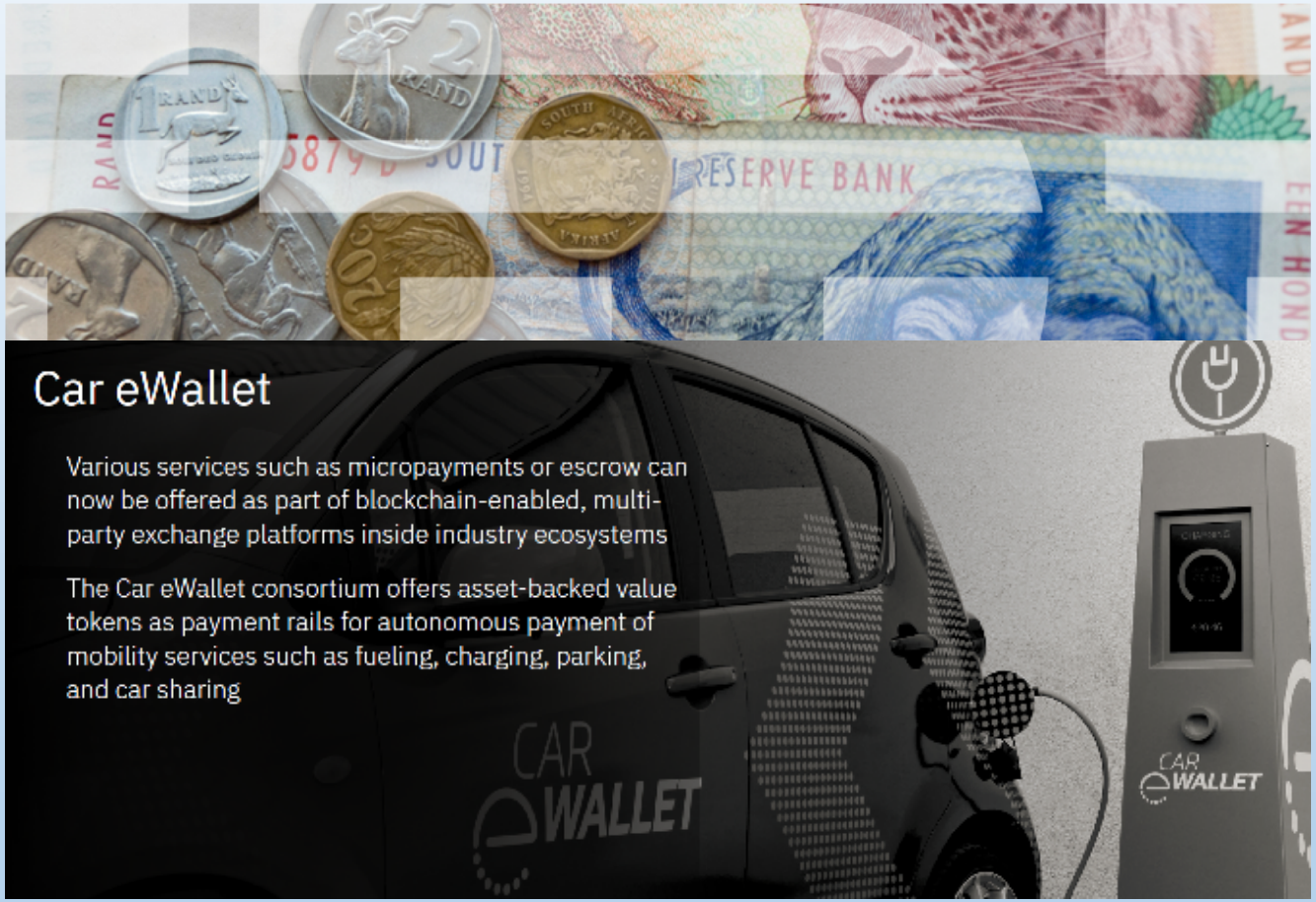
Distributed Ledger Technology (DLT) is changing cross – border payments with real-time smart, effective fraud management.

Data is helping extract payment information into unique insights, driving decision management.

Collaborative payment platform ecosystems with merchants, corporates, end-users/consumers is driving the future of payments.

New payment contactless, digital wallets and wearables channels gain consumer acceptance.

Tokenization with strong authentication and digital identity, biometrics and AI - is a new reality today.



Balancing Convenience and Security

Commerce – must be fast and easy.

Transactions – easy enable security measures.

Services support integrated loyalty.

24/7 functionality without security and data privacy breaches.

Pay as you go – real time transactions.

Effective Identity authentication with biometrics, tokenization, device fingerprints, AI to trigger fraud detection occurring real-time.

Complexity of Data flow

Understand customer preferences

Target buyers with tailored offers

Optimize supply chain

Anticipate product problems/warranty issues

Improve performance of enterprise assets

Detect/prevent fraud

The potential for insight is HUGE
but there are particular challenges to tackle … like privacy

Data can lead to incorrect conclusions, where privacy may be violated

Retails are attractive targets for fraud

Retailer	Damage	Means of Access
Neiman Marcus	350,000 payment cards	Malware implanted through outside attack
Michaels Arts and Crafts	2.6 million payment cards – 7% of all cards used at Michaels	Eight-month intrusion through PoS systems at some stores
Sally Beauty Supply	Company acknowledges 25,000+ payment cards exposed; outside estimates run to 282,000	Methods closely resemble those used in the Target breach
P.F. Chang's China Bistro	Customer data exposed at 33 restaurants	Targeted attack on PoS system

In H1 2017, 918 publicly reported cybersecurity breaches exposed over 1.9 billion records.

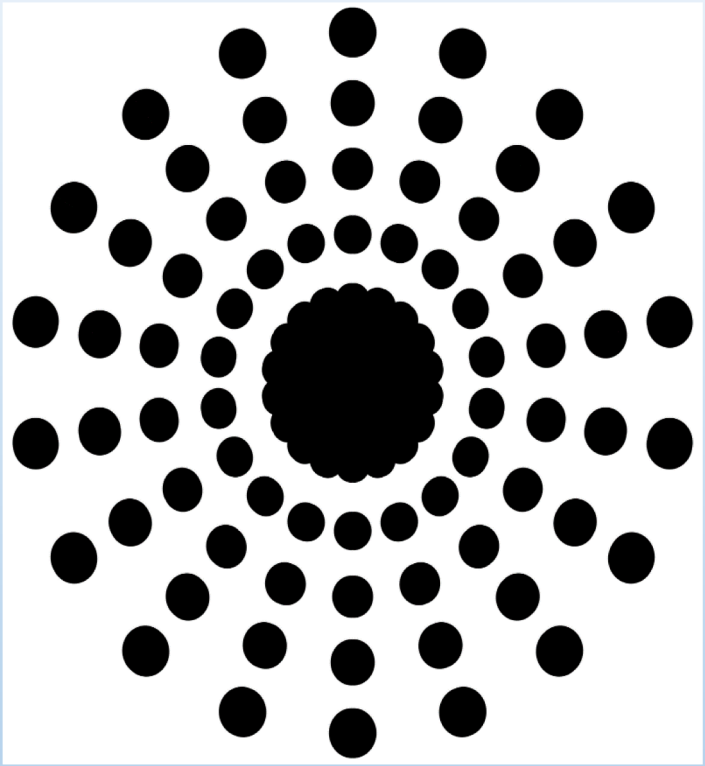
Prices for stolen credit card information range between $0.50 - $20. The price depends on the card brand, amount of metadata provided, volume discounts and how recently the card data was stolen.

The average cost of cybercrime attacks in USA is estimated at $12.69M. Estimates include detection, escalation, notification and after-the fact response such as legal, consulting, card replacement and credit monitoring fees.

*source – Ponemon Institute 'Cost of data breach Study'; Capgemini ' Top 10 Trends in payments 2018'

Evolution of fraud management

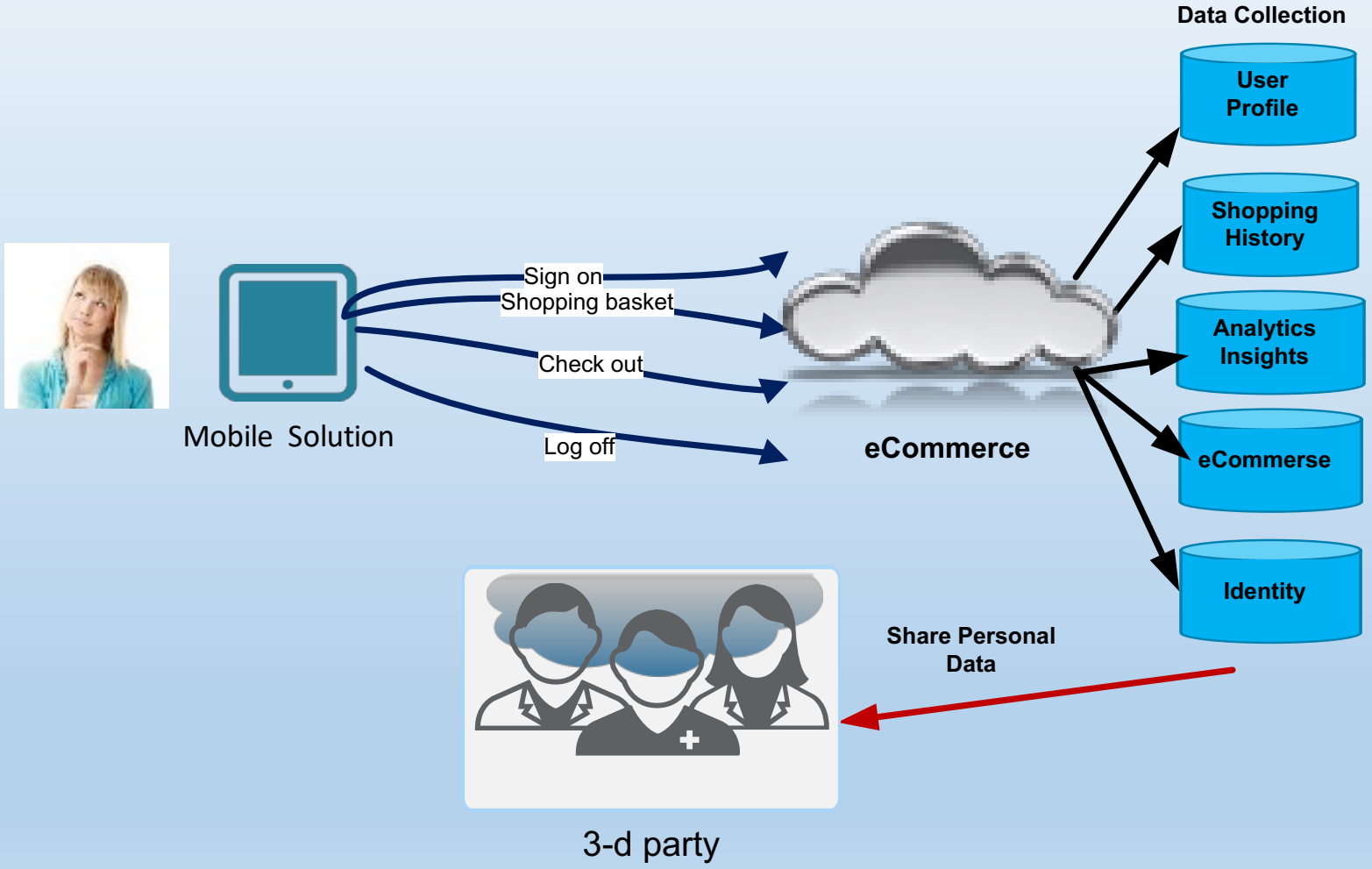
- Fraud management practices and systems need to evolve faster to counter increasingly sophisticated attacks.
- Fraud is a key thread to secure payments.
- Real – time payment ecosystem requires new approaches to fraud management.
- Effective identity authentication with fraud detection throughout the customer journey.
- Frictionless authentication and system of trust.
- Collaboration between account services and merchants for secure payments.



Security and Data vulnerability in IoT

- Privacy is one of the biggest legal challenges for the IoT
- Various apps and data centers' network outlets include high risk of DDoS attacks
- Implement mandatory authentication and access control for the access to the cloud is essential
- The various channels and devices for IOT transactions needs to be secure. With the world becoming more connected, retailers aim to tap into consumers' lives in a number of different ways:
  - Homes and vehicles become more connected through technology, making retailers challenging to provide a seamless transaction experience
  - Apps on smart televisions can be used to enable people to interact with retailers via their televisions
  - Smart store - Beacon technology can be used to navigate people around stores while capturing information about customers and their buying habits.
- Manage and care for consumers and merchants in the IoT Commerce world.
- Secure IoT commerce transactions and develop seamless IoT commerce

Data Privacy in the Consumer world



The issue of data ownership getting more complicated in the consumer world.

Older people, kids and other vulnerable population may not be aware that their location and other information is pushed back by their smartphones to their mobile provider or/and device maker.

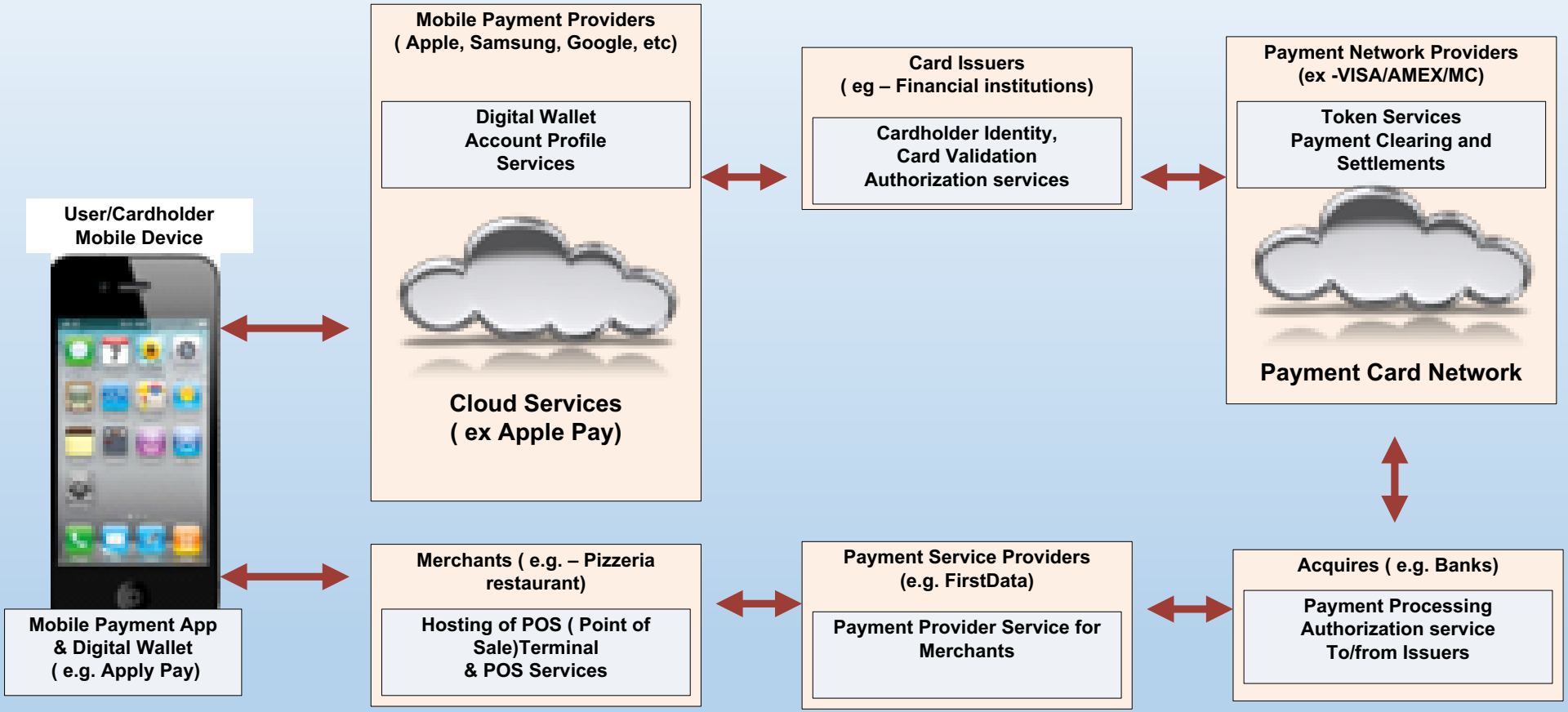
Data is collected in exchange to some special services, improved user experience. Data rights are lost…

How widely companies share the data

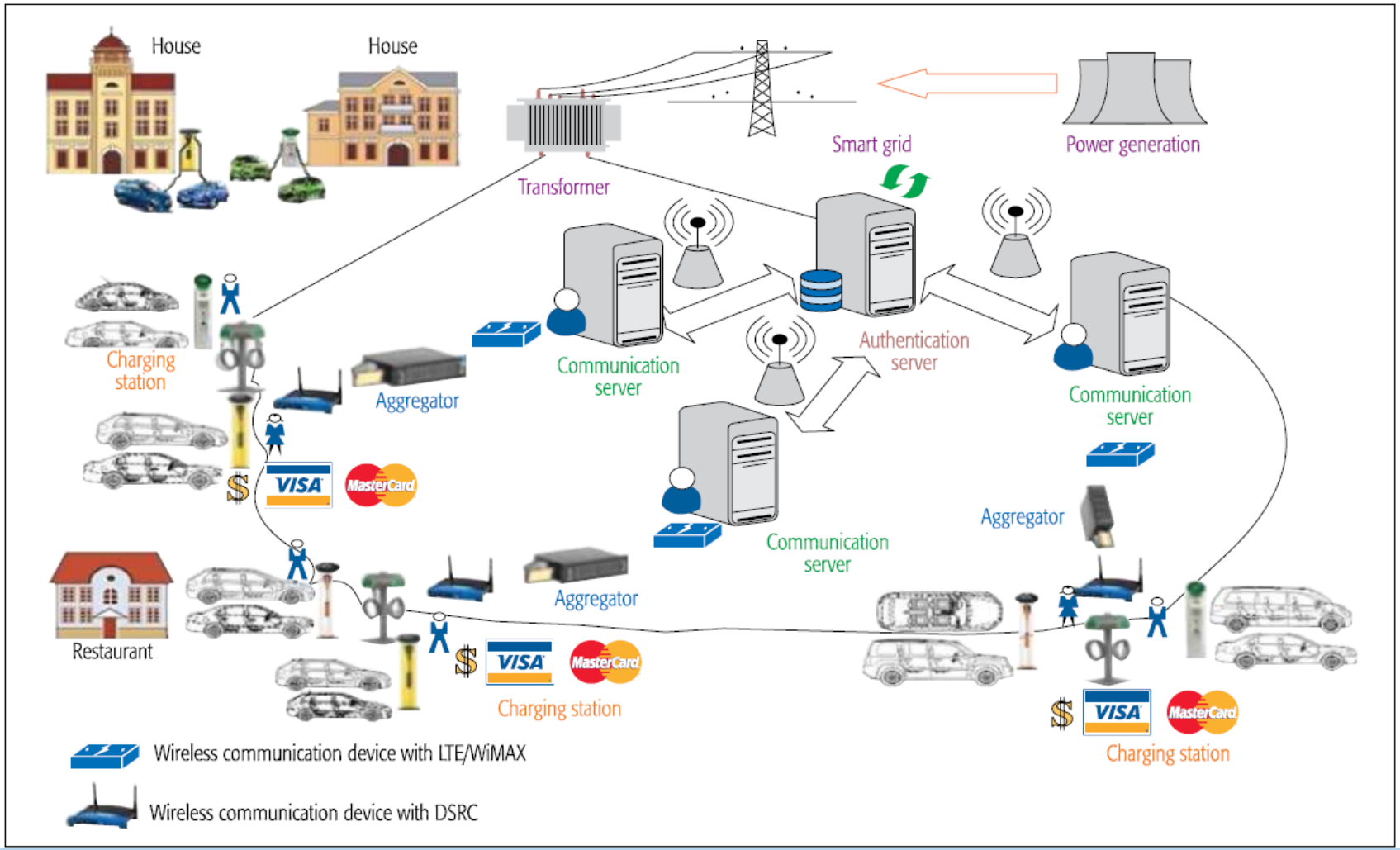
Source - http://rebecca-ricks.com/paypal-data/

https://www.paypal.com/ie/webapps/mpp/ua/third-parties-list

Threat Model of a mobile payment ecosystem



Smart Vehicle to Grid (V2G) challenges



The V2G network has a higher level of scale and complexity :

- technologies from several domains
- the diversity and large volume of stakeholders
- charging and discharging of the mobile vehicle's battery across centralized and distributed networks
- a secure payment system

Consumer data, such as specific times/locations of electricity use, type of operation requested, vehicles used, and other consumer behavior related data need to be protected when the utilities share consumer data with third-parties.

A V2G system is a cyber-physical system (CPS) consisting of interacting elements with physical input and output., not only dealing deals with information modification over the communication network but its effect on the power system.

http://eprints.bournemouth.ac.uk/28331/1/07880513.pdf

Key GDPR Aspects

'Even before the deployment of AI, we believe that organizations that collect, store, manage or process data have an obligation to handle it responsibly.'

https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/

Data Responsibility

Data Ownership and Privacy
A world being reshaped by the phenomenon of data requires clarity around the principles and rules of the road to ensure that the rights of those who own it and use it are protected

Data Flows and access
Commit to protect the privacy of data, which is fundamental in a data-driven society:

- Cross-border data flows
- Government access to data

Data Security and Trust
Protect global trade with the tools like AI and block chain
Address the need while striking the critical balance among security , privacy and freedom

Data and AI
Augmented Capabilities represent a positive and transformative force for business, institutions, governments and individuals, and must be developed in thoughtful and responsible ways

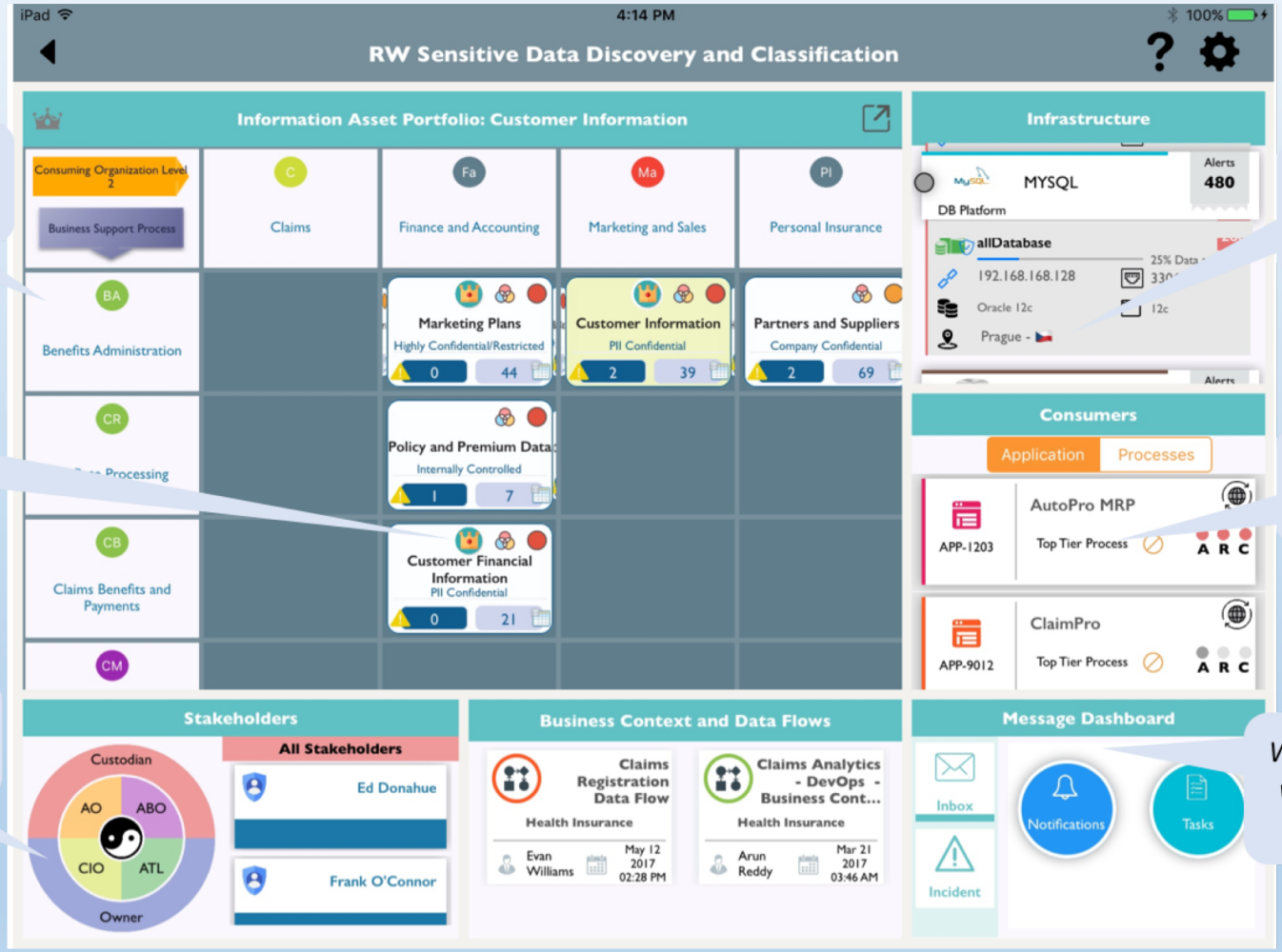
https://www.ibm.com/blogs/policy/dataresponsibility-at-ibm/

Visibility into critical data & potential risks

Which lines of business have the highest risk?

Are the "Crown Jewels" classified and protected?

Who are the owners of sensitive data?



Where does critical data reside? – Data centers and Geo's

What applications and processes access and use them?

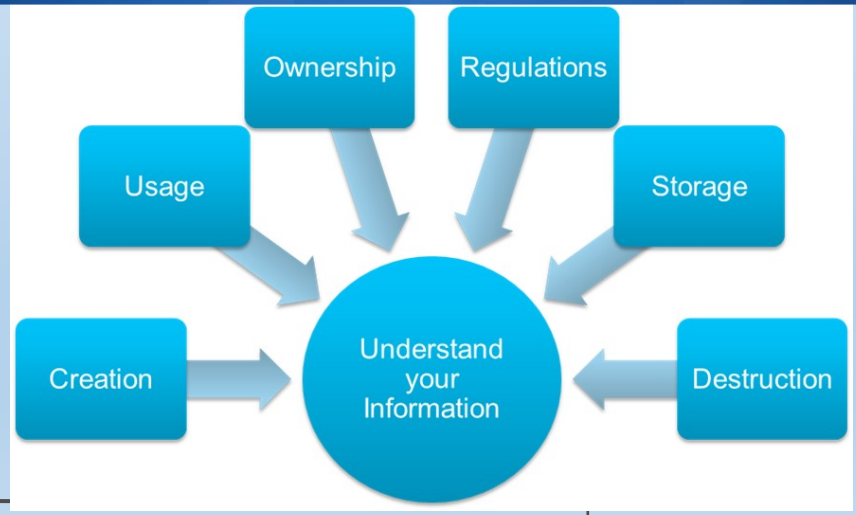
What compliance issues do we have and remediation action items?

Why we need better information governance?

To address today's business drivers, create a foundation of trusted data Develop a solid understanding of the following aspects of al of your information:

- ***Creation, usage, storage, destruction***
- ***Ownership & business responsibility***
- ***Laws and regulations***
- ***Effect and purpose of your data***

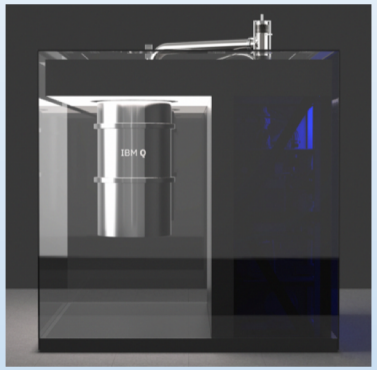
- Management of all unstructured data
- Master content management
- Management of both structured and unstructured data
- Content governance
- Content models and metadata
- Search and discovery
- Enterprise standards
- Analytics



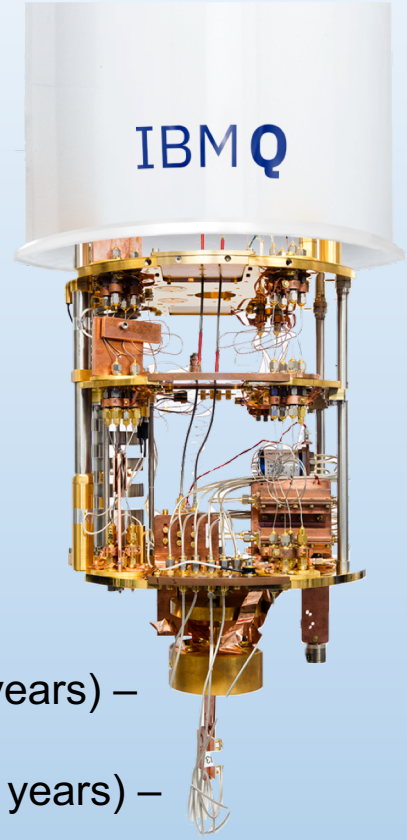
Quantum Computing – security threat?

Classical - Processing huge volumes of data and extracting insights
Quantum - Exploring an enormous set of possibilities for the best answer

VS



Products, services, business functions, that rely on security products, will either stop functioning, or not provide the expected levels of security. How soon to worry?



Depends on*:

- How long do you need your cryptographic keys to be secure? – *security shelf-life* (*x* years)
- How much time will it take to re-tool the existing infrastructure with large-scale quantum-safe solution? (*y* years) – *migration time*
- How long will it take for a large-scale quantum computer to be built (or for any other relevant advance)? (*z* years) – *collapse time*

"Theorem": If $x+y>z$, then worry.
*M. Mosca: e-Proceedings of 1st ETSI Quantum-Safe Cryptography Workshop, **http://eprint.iacr.org/2015/1075**

Assessing Threat

Assessing ‘x’

- Enumerate key information assets and business functions.
- Understand the nature of the systems being used (or that will be used), and the assets and functions they protect.
- Understand legal or regulatory influences.
- What is the value of those assets or business functions?

Assessing ‘z’

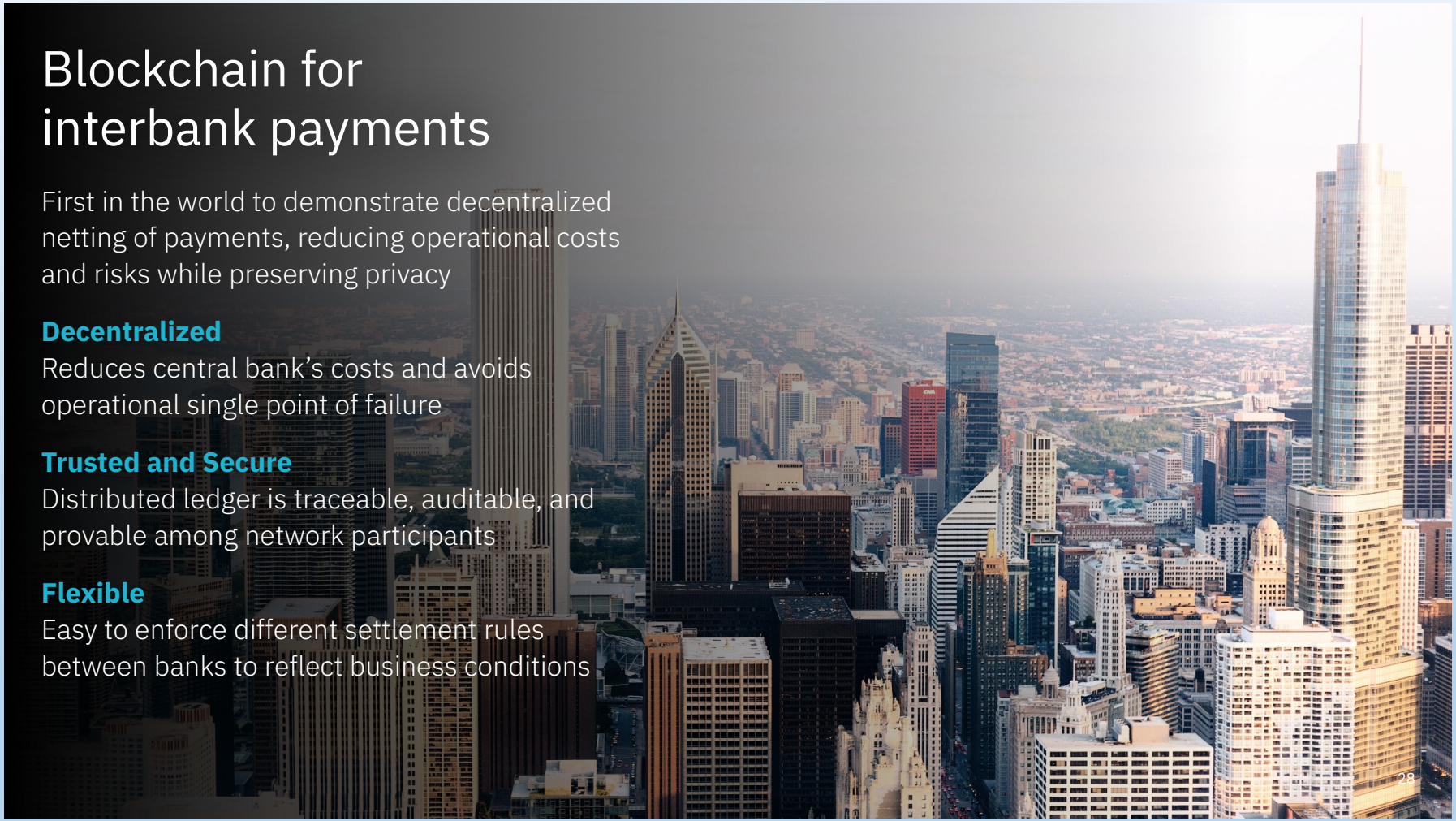
- Catalog system components and assess vulnerabilities to quantum attacks.
- Understand threat actors who might attack your systems.

Assessing and managing ‘y’

- Examine the existing risk mitigation policies, procedures, and processes, with a special focus on cryptography.
- Identify community and technical challenges to deploying quantum-safe cryptography.
- Natural approach is to integrate quantum readiness into current risk assessment/mitigation processes.
- As cryptographic tools and processes become scheduled for updates or replacement, consider quantum-safe technologies.
- Consider “hybrid” approaches to retain robustness of tools protecting against today’s threats while introducing new tools designed to protect against the future quantum threat.

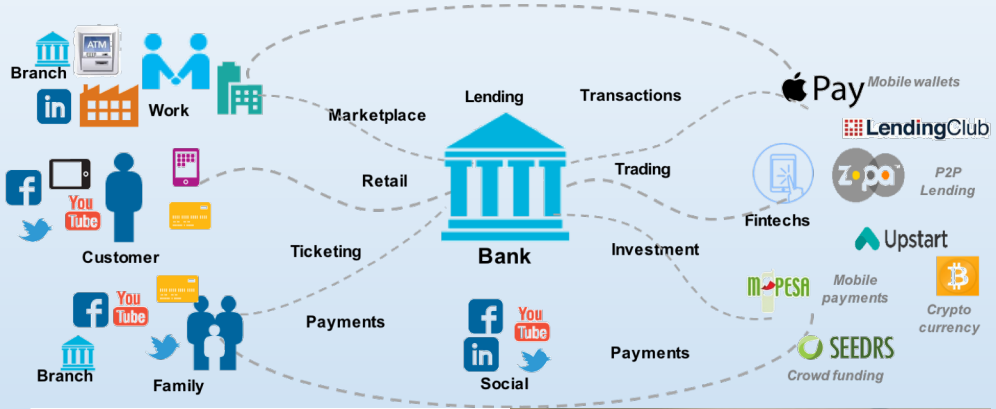
Obtaining specialized expertise and formulating a plan for your organization will help reduce losses and costs in the future

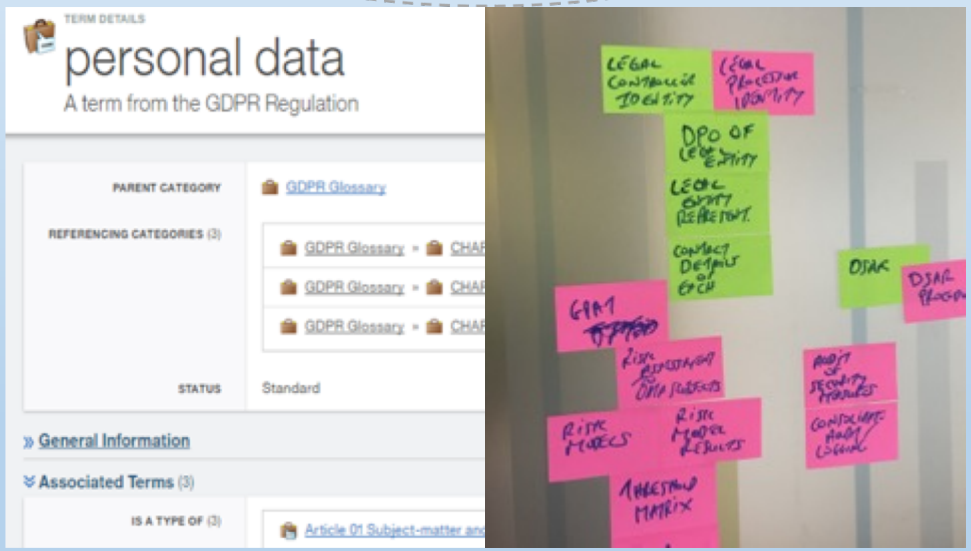
Blockchain


Blockchain for
interbank payments
First in the world to demonstrate decentralized netting of payments, reducing operational costs and risks while preserving privacy
Decentralized
Reduces central bank's costs and avoids operational single point of failure
Trusted and Secure
Distributed ledger is traceable, auditable, and provable among network participants
Flexible
Easy to enforce different settlement rules between banks to reflect business conditions
28

Design with the end in mind

- Ensure integrity and prevent from incorrect data being introduced during solutioning
- Provide capabilities required during the research and development phase to support design for security using technical standards
- Design governance training, communication & processes standard
- Design privacy, data management and security management standards
- Run benchmark test on non functional requirements
- Baseline statement of risks and threats for each component and subsystem
- Develop methods of testing the range of identified threats, individually, as modules, and as a complete system





Going Forward

- New disrupters are affecting customer relationships and business models
- Power dynamics of the industry are changing as people interact through new channels
- Future sector growth will be driven by a continuous increase in global smartphone use.
- FinTechs are gaining more power and are reinventing the payments industry.
- Instant payments are the fundamental building block for open banking.
- Understanding customers, predicting their needs and behaviors – continue to be the key.
- Regulatory compliance and protection from cyber crime will remain the highest priorities and will continue to be a challenge.

"If data is the new oil, then payment data is liquid gold" VISA October 2017