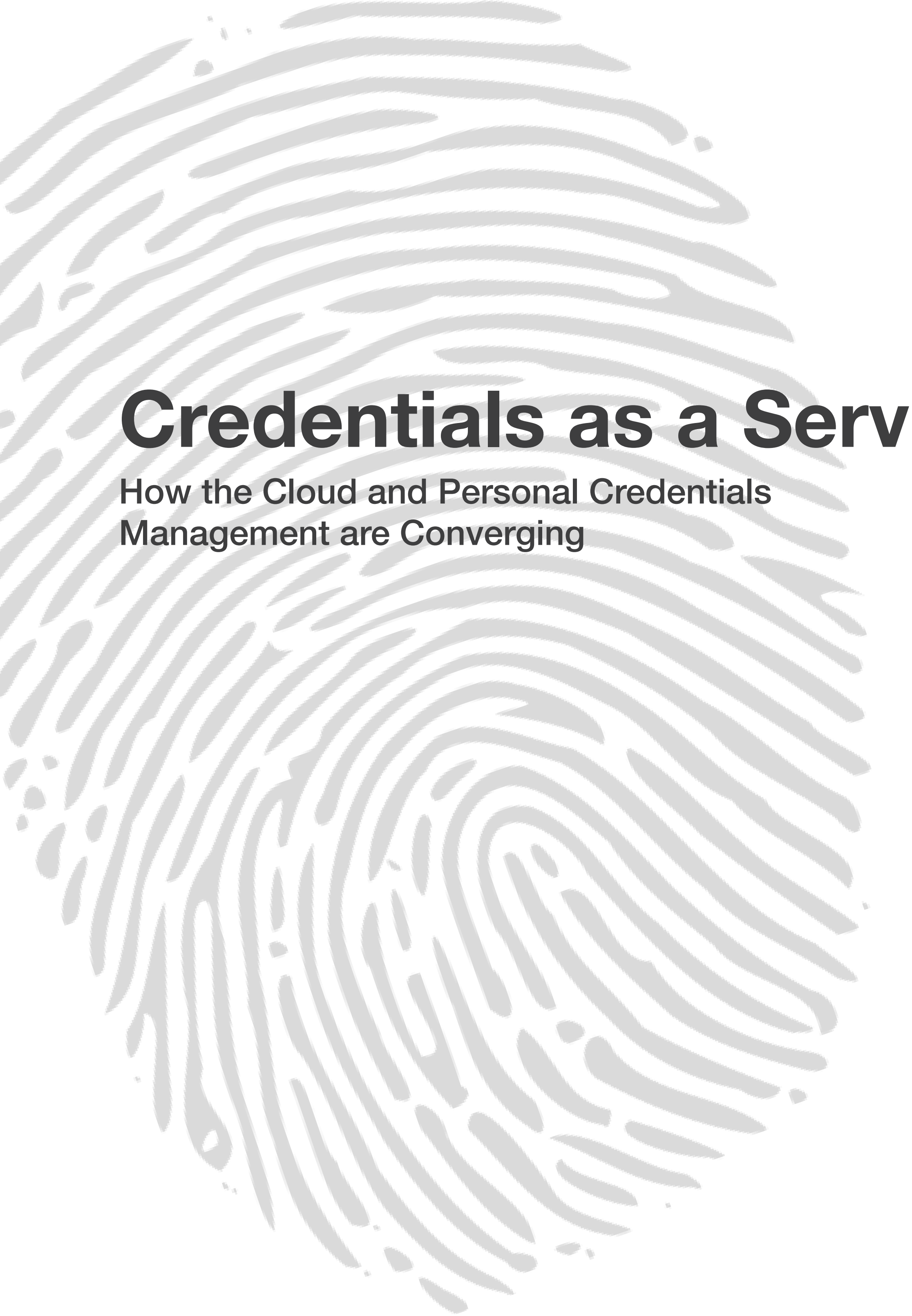
white paper



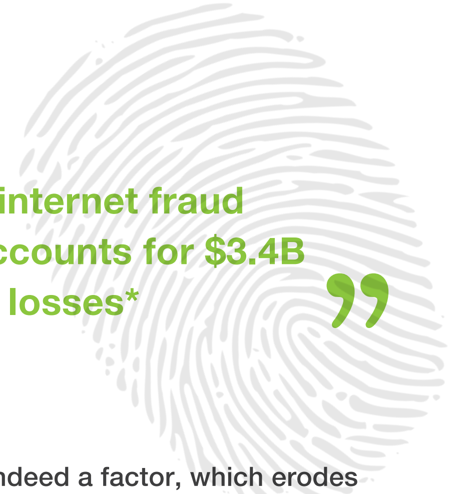
Credentials as a Service

How the Cloud and Personal Credentials Management are Converging

Nearly 25 years ago, Tim Berners-Lee, British software engineer and computer scientist, made his mark on civilization by creating what became known as the World Wide Web. His breakthrough was creation of a system that enabled computer users to share a common language to communicate over a network One networked computer could send another a set of data packets that would be assembled. Similar to letters one receives in the mail, each data packet carried the unique address of the receiving computer in the form of an IP address. However, unlike a typical postal letter, there was no addressee in the IP address. In fact, the person who requests and subsequently views the compiled data packets is, and remains to this day, completely anonymous. Had Mr. Berners-Lee augmented his original IP address construct with a “person identifier” the web would be quite different today.

“ **Credentials Defined: The token or tag that identifies a person to provide evidence for access to credit, confidence or authority.** ”

As it turned out, the anonymity of the web played a key role in fueling the rapid adoption of this new communications ecosystem and became the basis for an explosion in personal expression and commerce. But it also carried a dark side; the web’s anonymity provided a fertile ground for criminals to develop sophisticated ways to defraud businesses and consumers. Today, Internet fraud accounts for $3.4B in losses*, which ultimately find their way into the price of the products and services we all buy. Some of us pay an even higher price. It is estimated that 5% of Americans have their identities stolen each year and that often times leads to substantial losses and damage to the victim’s long term financial standing and reputation.



“ **...internet fraud accounts for $3.4B in losses*** ”

If anonymity is indeed a factor, which erodes the stability if not the very foundation of the web, it raises two questions: (1) Should the web be less anonymous? (2) How should the web be less anonymous? This analysis primarily tackles the second question, and asks the readers to draw their own conclusions about the first one.

* Source: Cybersource’s 2012 Online Fraud Report

The answer to how the web could be less anonymous is surprisingly concise, by authenticating people. That means developing a method for accredited individuals to present their credentials to conduct a variety of online transactions.

Though the phrase may sound a bit lofty, the meaning of presenting credentials is simply to provide evidence concerning one's right to credit, confidence, or authority. In the physical world we're accustomed to presenting our credentials to accomplish any number of tasks. For example we show a driver's license to cash a check or register at a hotel. We also show a loyalty card to earn a purchase discount or a student card for discounted admission. In web transactions, we're accustomed to entering our name, address, and credit card information in the checkout page of a retailer's mobile app or site. Though we present credentials with such frequency we hardly give it notice, it is the foundation on which most commercial and societal transactions are based.

CREDENTIALS: A BROADER VIEW

The range of credentials is many and varied though we tend to focus on two of them: Payment-related and personal identification-related. A credit card number is a payment credential while a state-issued driver license is used as an ID credential. Other documents are credentials in their own right. For example, an auto registration is a vehicle ownership credential and a utility bill is an address credential. While this may seem obvious from a linguistic perspective it is far from the reality of how credentials are accessed, stored, and used. Each credential is tied to its own ecosystem of issuance and usage, creating a hodge-podge of standards and practices.

> **“Each credential is tied to its own ecosystem of issuance and usage, creating a hodge-podge of standards and practices.”**

Payment credentials—the combination of credit card number, card owner name, expiration date and CVV number—represent the most widely used and evolved of any of the credentialing ecosystems. All participants, whether businesses, consumers, issuing banks, or credit card organizations, operate on the same set of rules that govern all elements of how transactions are conducted, reported, and disputed. Other areas of credentialing are far less developed and give rise to ambiguities. Is an address on a state-issued driver license considered proof of address? Does an insurance card prove vehicle ownership? On a more fundamental level, is the document even authentic?

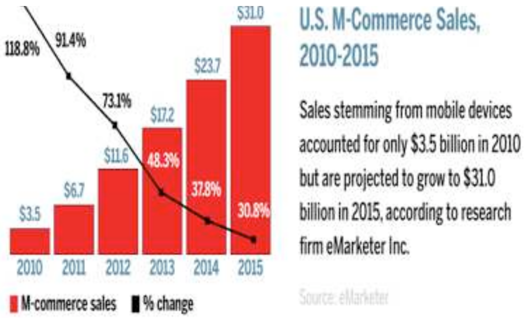
In online and mobile environments the same need to present credentials in order to conduct a transaction exists; however, the mode of presentation is more varied and far less efficient than in face-to-face situations. In ever increasing numbers, we routinely use these remote access modes to open accounts that require a tax identification or social security number, and often we are asked to simply attest that we are authorized to engage in a process since there is no practical way to ascertain it for certain. We encounter this when placing an order from an online wine shop or gaining access to certain gaming sites. In these instances we're on the honor system and simply attest to our age and jurisdiction to complete the transaction even though there is no mechanism to provide an actual credential.

When opening financial or other regulated accounts, the most common practice is to require the consumer to mail, fax, or physically deliver the requested credential to complete the transaction. Aside from the obvious impediment this represents to rapid transaction completion, it's also expensive for merchants to process credentials in this manner. The simple act of receiving, reviewing, and filing a faxed ID is estimated to be over $25. The quality of validation is also suspect since the there is no source document to review, only a lower quality fax or copy. If a deeper set of information is required, such as validating a job seeker's education credentials or other background checks, the costs can easily escalate up to $1,000. This of course does not include the actual fraud losses that a business may incur by allowing a criminal to slip through their control processes.

ID verification technology circa 2013.

Businesses have a lot more to consider than just cost. How is the customer data being handled, who sees it and has access to it? How secure is the data storage and how frequently must the customer record be accessed? While processing cost is always relevant, the issues these questions raise make the issue of cost pale in comparison.

WHY MOBILE CHANGES EVERYTHING



U.S. M-Commerce Sales, 2010-2015

Sales stemming from mobile devices accounted for only $3.5 billion in 2010 but are projected to grow to $31.0 billion in 2015, according to research firm eMarketer Inc.

Source: eMarketer

Mobile device usage is exploding and so is the frequency of conducting transactions on our smartphones and tablets, which used to be the sole domain of the desktop computer. Over the next 3 years, m-commerce is forecasted to grow at a nearly 40% year-over-year pace and reach a $31 billion in US sales volume by 2015. Of course, that represents solely purchases and not the myriad other tasks we regularly accomplish such as applying for mortgages, trading stocks, and more. On any street corner in nearly any city in the world it's now commonplace to see people of all ages interacting with their devices as they walk by. There's even an app that allows users to see the sidewalk just ahead while they busily engage with another app. No matter what the actual mobile usage growth rates turn out to be, we all know that mobile access has changed the way we conduct ourselves during our waking hours.

Mobile access has become fundamental to daily life.

Increased mobile usage brings with it three new design and usage paradigms:

1. **Smaller form factor:** Mobile devices, even tablets, are not small PCs. They represent a completely different user experience from the desktop and as any app developer will tell you, shrinking a desktop experience to a smaller device is a surefire way to create a poor user experience. As the mobile era unfolds we are seeing new mobile UI de facto standards emerge just as we saw new site design standards for web design in the heyday of Web 1.0. However, new user paradigms are lagging on transactional pages, most notably on ecommerce checkout, which still requires users to key enter personal information and credit card numbers by hand. For credit card entry alone, the average mobile consumer requires 3 tries and nearly 60 seconds to get it right. The negative impact this has on transaction completion cannot be overstated. Consumers require a more automated – and secure – way to share personal credentials at this all-important point-of-transaction.
2. **New Security Risks:** Cyber-criminals most actively ply their trade on the newest forms of access since those are being developed and adopted so quickly that security standards often lag. Mobile is no exception in this regard, even though mobile devices are easier to ID than desktops other factors such as network security come to play. In fact, Javelin Strategy found that smart-phone users experience a fraud incidence rate one-third higher than those that don't own smartphones. The fact that there tends to be a one-to-one relationship of user to device, (unlike a desktop PC which may have many users) is a strong point for security, but standards, protocols and user behaviors are still evolving, creating a wide array of fraud holes that cyber criminals are the first to identify and exploit. Many consumers still connect to unsecure Wi-Fi networks with little recognition that their personal data can be easily captured in that setting.
3. **Attention Deficit Design:** Mobile users are just that ... mobile. As obvious as that is, it has serious ramifications on transaction processes and design. Unlike sitting at a desktop where our feet are firmly planted on the ground and our attention is largely given to the task at hand, mobile activity, whether on a smartphone or tablet, competes with numerous elements that require our real-time attention. Walking, navigating traffic, people watching in cafes, any form of multi-tasking are the norm and often require one-handed device operation. The usage paradigm is such that well-designed app processes are adapted towards a "low attention" environment. This notion of attention deficit design is broader than solely simplifying data entry and other checkout screens. It also addresses the role that tablets play compared to smartphones – the former's larger form factor facilitates data entry but regardless of the device used we're splitting our attention in new and varied ways.

Attention fragmentation is becoming the norm.

THE MOTHER OF ALL CREDENTIALS

Certainly the most frequent instance of credential presentation is when we authenticate ourselves in order to gain access to the multitude of password-protected sites we engage with on a daily basis. Email, ecommerce, stock brokerage, and home banking are just a portion of the sites we use for a wide variety of purposes and transactions. Presenting credentials in this instance takes the form of typing in the ubiquitous username and password.

The first and last line of defense?

Once access is gained, we generally have free run; able to make account changes, move money, purchase items, close accounts, communicate with our friends and more. Perhaps, more than any other credential, username and password provide the keys to your personal kingdom. Since username and password are the sole line of defense against those who would like to steal your ID, money, and reputation, surely this credential ecosystem must be the strongest of any in use today.

THE PASSWORD CRISIS

Regrettably, nothing could be further from the truth. Simply put, the passwords we create are not secure, and even if they were, the businesses that store our passwords and other personal data are not, in general, sufficiently secure either. With alarming regularity we learn of huge data breaches at some of our finest and most respected companies. In fact, DataLossDB found over 1,000 data breach incidents in 2011 alone.

> “...identity theft in the US now afflicts 5 percent of all Americans annually and ecommerce merchants absorbed more than $102 billion in fraud...”

We consumers have not been helping matters either. The majority of us engage in very risky password behaviors. Nearly 60% of consumers use the same password on multiple sites, and the same number choose passwords based not on their security features but for easy memorability. Once a single site has been breached, the likelihood that all sites that use the same or similar password can be breached increases. So while it may seem unimportant that a secondary retail site you only use occasionally was breached, it could mean that your brokerage or email account is now open to cyber criminals. That’s why identity theft in the US now afflicts 5 percent of all Americans annually and ecommerce merchants absorbed more than $102 billion in fraud related losses in 2011. We should expect to see these numbers grow faster than the growth in online and mobile commerce in coming years due in no small part to the accelerating growth of mobile transactions. Mobile, being the new frontier, has opened up a new set of fraud holes that the criminal element has successfully identified and exploited.

Internet fraud accounts for $3.4B in losses.*

* Source: Cybersource’s 2012 Online Fraud Report

RISKY BUSINESS: THE PARADOX OF RISKY BEHAVIOR

> “...89 percent of us think our password practices are just fine.”

When we are about to engage in risky behavior in one form or another, we tend to evaluate risk on the initial instance of that behavior. If we choose to go forward and there’s no negative consequence to our action, the likelihood that we’ll continue to engage in the behavior increases. The paradox is that with each subsequent event our perception is that the risk is reduced – after all, we’ve done it before without consequence – while in fact, the opposite is quite true. Even if each action is discreet and statistically unrelated to the prior one, the frequency of action gives rise to complacency which in turn increases risk. Intentionally driving through a red light the 100th time is as risky as doing it the first time, but habituation reduces caution and that also increases risk. Even if each risky behavior is unrelated statistically to the prior instance, the risk is additive. The person who drives through red lights every day is more likely to eventually have a resulting accident than someone who does it once a decade.

Now apply this thinking to password settings and it’s easy to understand that despite the fact that the majority of us engage in unsafe password practices at some point, we reused a simple password on another site and nothing negative occurred, so we did it again and again, and still nothing bad has happened. This, of course, perpetuates the behavior and increases complacency. The paradox is alive and well.

Don’t try this this at home.

CONVENIENCE: CULPRIT OR KING?

As a fellow consumer, it’s easy to understand how we got here. It was all very innocent… we were shopping online and at the checkout filled out our personal and credit card information. Then we saw a checkbox labeled “remember me” or a suggestion to open an account which at that point required only setting a password. Of course, we have to set a password we’ll remember so we default to the one we use all the time. Perhaps we have two often-used passwords, one for “important” sites like home banking and one even simpler password for infrequently used sites or apps like the particular retailer in this example. How convenient to enter an oft-used password and forget about it until the next time you happen to shop there. The end result is that our personal credentials are stored all over the web and the keys to one site are likely able to open another and another.

Online retailers are not the source of the problem but certainly play their role in the password crisis. The retailer’s consideration is all about repeat business; now that you’ve shopped once on my site, my very reasonable business objective is to make it easier for you to shop again. But in order to accomplish this, online retailers offer you the convenience of storing your personal and payment credentials. Surely they considered all aspects of security, password strength, and meet all the most stringent standards. Again, not quite so. Only 28% of US small businesses have a formal Internet security policy.

> “PCI compliance is complex and expensive and more suited to a techno-bank than a Halloween costume online retailer.”

Meeting industry credit card storage requirements (a portion of PCI compliance) is a complex and expensive set of security requirements more suited to a techno-bank than a Halloween costume seller. Prior to this compliance requirement, online retailers stored your payment and personal credentials in any manner they saw fit – and the integrity of those systems spans the gamut. Regulations pertaining to storing customer credit card data are only one piece of the best practices and regulatory puzzle. Considering the costs of compliance on one hand and the cost of data breaches on the other, businesses of all sizes should approach this topic with a great deal of consideration.

If you outsource the handling of cardholder data to a third party service provider, verify that they have validated PCI DSS compliance and are listed on Visa's website.

PCI compliance checklist for businesses storing consumer credit card info*:

BUILD AND MAINTAIN A SECURE NETWORK

Requirement 1: Install and maintain a firewall configuration to protect cardholder data

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

PROTECT CARDHOLDER DATA

Requirement 3: Protect stored cardholder data

Requirement 4: Encrypt transmission of cardholder data across open, public networks

MAINTAIN A VULNERABILITY MANAGEMENT PROGRAM

Requirement 5: Use and regularly update anti-virus software or programs

Requirement 6: Develop and maintain secure systems and applications

IMPLEMENT STRONG ACCESS CONTROL MEASURES

Requirement 7: Restrict access to cardholder data by business needto know

Requirement 8: Assign a unique ID to each person with computer access

Requirement 9: Restrict physical access to cardholder data

REGULARLY MONITOR AND TEST NETWORKS

Requirement 10: Track and monitor all access to network resources and cardholder data

Requirement 11: Regularly test security systems and processes

MAINTAIN AN INFORMATION SECURITY POLICY

Requirement 12: Maintain a policy that addresses information security for all personnel

* Source: PCI Security Standards Council

DATA LIABILITY

Businesses recognize a wide range of liability issues; from in-store consumers slipping on a wet floor to insurance to protect the personal assets of corporate officers should the business be hit with a legal action. With the rise of stored data and cyber crime customer data, ownership has now become a business liability like any other. The stakes are high: in most cases businesses are liable for credit card fraud in card-not-present transactions and financial institutions and other businesses must be in compliance with a complex set of rules and regulations such as the Anti-Money Laundering act (AML), which is designed to crack down on transfer of illicit funds around the world. In 1996 the International Monetary Fund estimated that between two to five percent of worldwide funds transfers were illicit – and though it’s difficult to measure this it certainly accounts for billions of dollars today.

Most forms of business liability are unavoidable; a retail outlet can’t operate without floors for customers to walk on even though they may slip and be injured on those floors. But in the case of customer credentials storage, this form of liability is largely taken on voluntarily by many businesses. The reality is that retailers don’t really want to store your credentials, it's just a necessary evil in order to achieve the goal of providing consumers with transactional convenience - a goal most consumers embrace. Astute businesses realize that they don’t need to store customer credentials and other personal data, they just need access to the stored data. The question is, by what other means may businesses provide the same level of consumer convenience without placing the consumer and the business at risk?

> **“Businesses don’t need to store customer credentials; they just need access to them.”**

The answer to this question opens up a whole new way of thinking about credentials and lays out a framework for developing systems that are far safer than those in use today without sacrificing the conveniences that we demand. The answer is in the Cloud.

THE ANSWER: CREDENTIALS as a SERVICE (CaaS)

In light of the situation and risks outlined above, it's become apparent that businesses need to adopt a more secure and holistic way to ensure that their customers are able to enjoy convenient and safe transactions. Envisioned is an independent service that provides on-demand and pre-authorized access to customer credentials absolving businesses of the tasks of collecting, verifying, maintaining, and serving the credentials at sign-in and other points of transaction.

The perfect storage platform
for easy access and safe keeping.

Having these solutions be tied to a specific merchant or even a credit card organization is too limiting, as the solution must embrace all transactional credentials and be non-partisan.

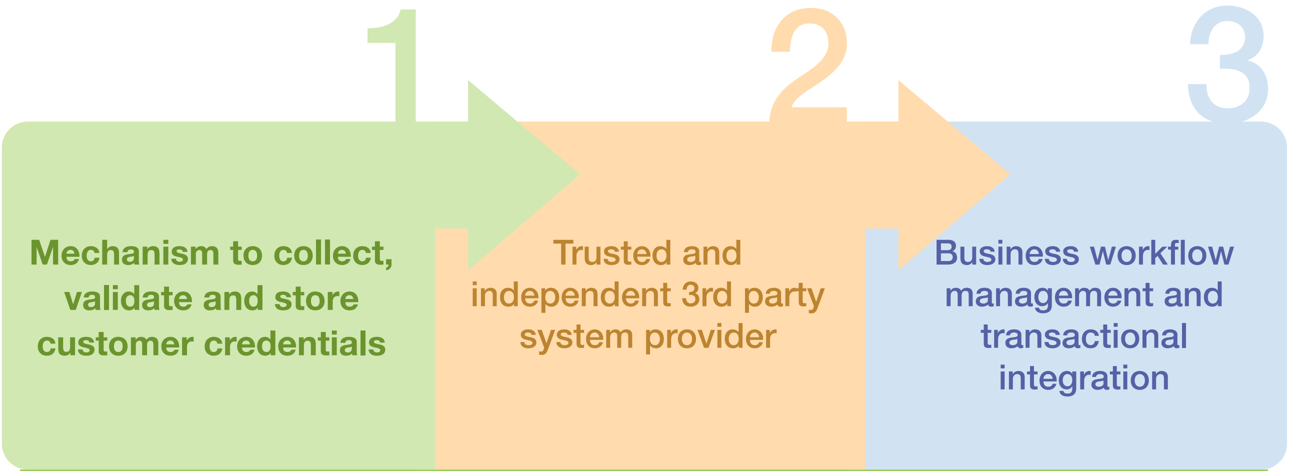
CORE COMPONENTS OF CREDENTIALS as a SERVICE SYSTEM:

Imagine these common use cases:

- A US consumer wishes to open an online brokerage trading account to write some options calls.
- A British consumer wishes to play online poker to hone her poker skills prior to a trip to a Macau casino.
- Using a peer-to-peer marketplace, a vacation homeowner wishes to rent his property to a French tourist he doesn't personally know.

How can these transactions be conducted in a way that provides trust and security to the businesses but are not so cumbersome and invasive that it causes consumers to bolt? What are the components and functions of a system that can achieve this balance and act in both party's best interests?

A COMPREHENSIVE CaaS SYSTEM IS COMPRISED OF 3 DISTINCT ELEMENTS:



1 Mechanism to collect, validate and store customer credentials

2 Trusted and independent 3rd party system provider

3 Business workflow management and transactional integration

1. A mechanism to collect, validate, and store consumer credentials.
2. A trusted 3rd party system operator to validate, hold, and present the credentials on behalf of consumers in specifically defined instances.
3. A mechanism to provide businesses with workflow management so they may easily set which credentials are required for each business purpose. This aspect also demands seamless integration into the business' transactional flow.

9 CHARACTERISTICS OF A COMPREHENSIVE CaaS SOLUTION:

Software as a service (SaaS) delivery systems have gained great popularity in recent years. As a general business model SaaS delivers the key benefits of rapid and inexpensive start-up costs, variable pricing often times based on a “pay as you go” pricing model and anywhere, anytime access for system users.

1. **Verified: Consumer credentials must** be verified before they can be used in transactions. If fraudulent data is allowed to enter the system then the system will be subject to fraudulent transactions.
2. **Secure:** Credentials must be stored and transmitted in a way that meet the most stringent data security requirements and applicable regulations and best practices.
3. **Independent:** The CaaS provider must be an independent entity not in competition with any of the companies who use the service. However, it need not be a governmental agency, and a strong case may be made that it should not be a governmental agency due to the geographic and political limitations that would impose.
4. **Configurable:** The CaaS system must provide business users with a fully configurable control system that enables the business to determine which credentials it wishes to access in which circumstances and geographies.
5. **Data Retrieval:** The system must allow for easy retrieval of relevant credentials information at any point in the transaction lifecycle.
6. **Consumer Centric:** Consumers must be aware of what data is being stored on their behalf and control what information is shared in each and every transaction instance. Consumers must be able to easily edit and update information on file.
7. **Business-Centric:** While being both consumer and business centric concurrently may seem like a contradiction it is a requirement of a successful CaaS system. Businesses require a consolidated interface through which all matters pertaining to their customers’ credentials can be managed. This control panel is particularly important when the businesses choose the highest security setting of not storing any credentials information.
8. **Transaction Friction Minimization:** Consumer-facing processes at the point of transaction must be designed to eliminate transaction friction, not add to it. All processes must conform to stringent mobile user interface requirements.
9. **Demonstrated Value:** The value provided in the form of increased transaction completion and reduced chargebacks and fraud must exceed the cost of using the CaaS system.

2013: THE END OF “CUSTOMER OWNERSHIP?”

Both currently and historically, businesses have viewed customers with whom they do business as assets that they “own.” Any enlightened business executive will deny this and acknowledge that the business must earn the customers’ loyalty by providing value and being responsive to their needs. Yet there still persists a belief that the business that “acquired” the customer owns him. And what this really means is the businesses think they own their customers’ data and the right to communicate with them. The language we use speaks volumes. We target, acquire, and retain customers just as we do military targets.

If you value customers, set them free.

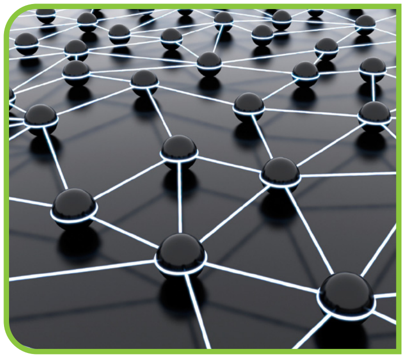
However, there are two broad classifications of data that businesses hold. On the one hand, there is transactional data reflecting customer purchase patterns or other preferences which most would agree that the business does own. That data wouldn’t exist unless the business took measures to track and analyze their customers’ behavior. It represents a competitive advantage to put this data to good use, and the more value they can derive from this data the better it is for businesses and arguably consumers. Using this data allows for astute businesses to customize offerings for each customer and even determine what unique content to place on the next page of the company’s website during a shopping session.

The other classification of customer data is much more narrow and describes personal credentials such as payment, identification, geo-location or anything that enables the consumer to conduct transactions.

Too many businesses have conflated the two forms of customer data and see them as one. With the advent of Credentials as a Service (CaaS), it’s now possible – and advisable – for businesses to divest themselves of customers’ personal data as they neither have ownership rights to it nor do they wish to carry the liability associated with storing such data. The usefulness of personal credentials data as a component of various business processes is not in question. But a shift in thinking is upon us that recognizes that there is negative value in owning the data when all the business wants or needs is access to it.

THE POWER IS IN THE NETWORK

CaaS offers significant value within the “walled-garden” of any single business. Imagine the benefits of eliminating data liability, knowing that the data is real, verified, and providing a holistic way to manage customer permissions and other operational details. But the real power of a CaaS system is found in the network of business and consumers who embrace the solution.



The power is in the network.

When businesses contribute their customers to the network they acquire the capability of instantly knowing transactional credentials of any network customer who comes to their site or app even if it is a first time transaction. This describes the ultimate frictionless transaction. The consumer carries their own “passport” wherever they go and, in combination with the CaaS provider, makes credential information available to merchants and other businesses. “Walled garden” solutions will never provide that functionality and will ultimately fail because the consumer will come to expect a universal standard and process. Imagine if every telephony provider operated a closed system that forced callers to dial a number unique to their system in order to reach the intended party. Thankfully, the standards are such that anyone can call anyone else on the network regardless of who is providing their telecom service.

In this critical regard, CaaS differs from most other SaaS offerings that are designed to operate in a closed system. Salesforce.com provides a powerful service that companies use for lead management, sales force automation and CRM functions. Marin Software offers a paid search SaaS solution enabling PPC advertisers to manage large and complex campaigns. File storage and access providers make it easy for customers to “rent” centralized storage and access for company documents. None of these leading SaaS providers create a network of users that by virtue of the network participation create a higher degree of value for all participants. While a CaaS system provider could offer each distinct business a better way to manage their own customers’ credentials, the real power of the system is in the network.

WHAT OF THE MOBILE WALLET?

There is perhaps no digital product concept that is more confusing to consumers and businesses than the “mobile wallet”. The term is becoming more commonplace in consumer vernacular; nearly two out of three respondents to the survey (65%) told the Pew Internet & American Life Project that they think most people will have fully adopted the “mobile wallet” as their day-to-day means of paying by 2020. Yet, it seems that there are as many definitions for it as there are providers, which by some counts is in the hundreds. The common element of most fledgling mobile wallets is that they are payment apps that enable consumers to use their smartphone or tablet to draw on stored funds or access credit/debit cards in order to make a point-of-sale purchase. Perhaps the moniker “wallet” overreaches and is the source of consumer confusion? After all, the actual wallet we all carry provides much more functionality than just being a payments facilitator. It does hold our payment mechanisms; plastic and cash, but it also holds our ID, vehicle ownership, health care access, insurance, employment, and any other credentials we use to conduct our daily transactions.

Our goal is not to contribute to the general confusion swirling around mobile wallet apps and terminology; however, the reader will recognize that a robust Credentials as a Service offering delivers the consumer the full functionality of a true wallet that is designed to conveniently access all payment, ID, and other credentials to facilitate not just mobile, but any online transaction. The other key distinction is that CaaS provides the business with complete backend functionality to holistically set business rules and manage all collection, verification, reporting, and access to customer credentials.

Should your digital wallet do less than your real wallet?

Consumer adoption of mobile wallets (aka payment apps) is still in low single digits—only three percent of smartphone users, 2.7 million Americans, have made a POS mobile payment—but eventually will find a loyal and sizable market, as the number is expected to grow to 48.1 million Americans by 2016. We believe this will occur when these wallets begin to add value beyond solely acting as a new payment alternative to use instead of credit/debit cards or cash at POS. The enabling technology is not the wallet app per se or its transactional integration, rather it is the ability to access and present consumer credentials in the manner described in this white paper.

WHAT THE FUTURE HOLDS

In this document we've laid out the foundation for why we expect to see significant evolution in relation to how personal credentials are managed by businesses and consumers. We believe that change will manifest itself over the next five years in the following ways:

1. The practice of businesses storing customers' personal credentials will be supplanted by one or more cloud-based credentials management systems.
2. While companies such as Apple, Google or Amazon have the customer footprint, trust and technology savvy to build and operate such a system, the CaaS system that will gain dominance will be operated by an independent third party that does not compete with any of its users' partners.
3. Losses in brand reputation and other assets from actual data breaches and broader recognition of potential liability will cause most reputable businesses to actively divest themselves of holding sensitive customer data.
4. Service-oriented companies will uncouple customer loyalty from customer credentials "ownership" without sacrificing transactional ease. Early adopters of this viewpoint will be heralded as customer relationship leaders and set the industry benchmark for others to follow.
5. A critical mass of online and mobile businesses will earn the right to display a recognized symbol of "no customer data stored" thereby eliminating their site or app as a target to cyber criminals. Non-compliant businesses will, however, experience a more concentrated level of criminal threat.
6. Personal authentication will become the prevalent transactional standard as opposed to payment card or device authentication.

However things ultimately evolve, we hope that this white paper helps to define the issues and opportunities that govern credentials management and provide a thought provoking blueprint for the next stage in online and mobile development.

About the author:

Marc Barach is CMO and head of strategy at Jumio. Utilizing advanced computer vision technology. Jumio is a next generation credentials management company offering mobile and online payment and ID validation products designed to reduce fraud and increase revenue by minimizing friction in customer transactions. Jumio's products are widely used by leading retailers, marketplaces and financial institutions. The company is backed by top-tier investors Andreessen-Horowitz, Citi Ventures and Facebook co-founder Eduardo Saverin. Headquartered in Palo Alto, CA, the firm operates globally with offices in the US and Europe.

Please contact us at sales@jumio.com to learn more or follow us on Twitter @jumio.