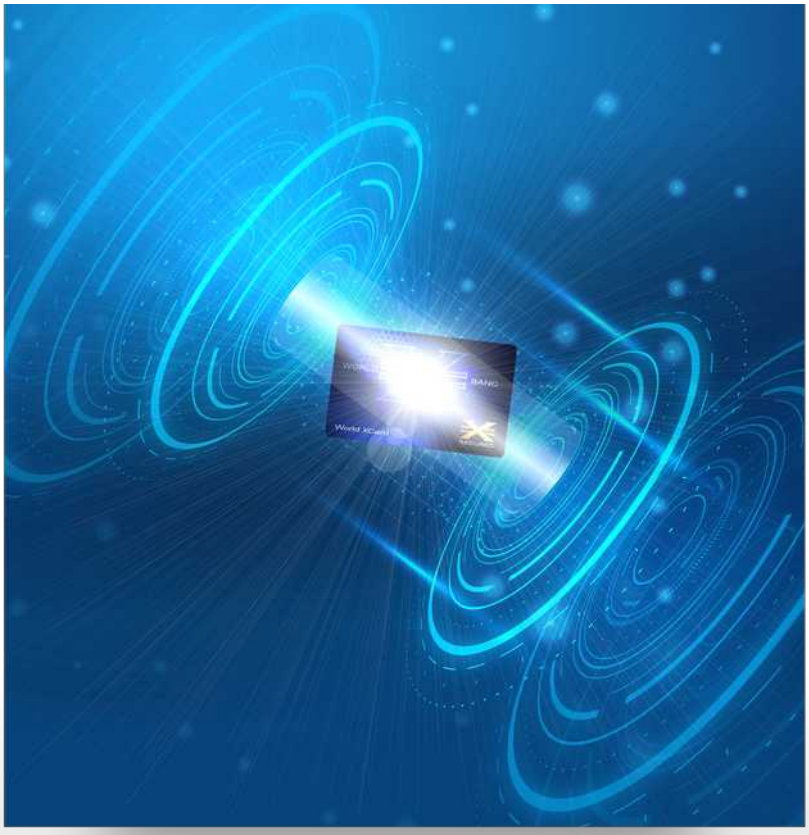
WHITEPAPER



Breaking Fraud

The Reality of Fraud-Proof Payments

WORLD X PAY

Cover image credit: Rosario Laperal, vecteezy.com

World XChange Inc.
PO Box 7492
Loveland, Colorado 80537 USA
833-473-XPAY
world-xchange.com

Table of Contents

OVERVIEW

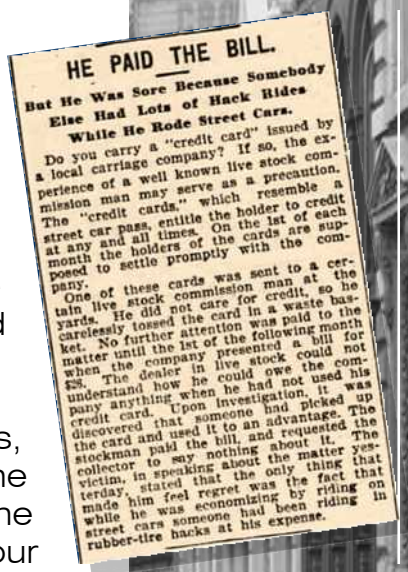
The issue of credit card fraud is so pervasive in the world that all attempts to solve it seem to have been abandoned in exchange for strategies to merely minimize it.

This whitepaper will identify the true causes of payment card fraud and subsequently explain why all security measures to date have failed to stop it.

Due to this misidentification of the cause, the vast majority of so-called solutions fail to protect everyone involved in a transaction equally. More often than not, the merchants are the ones left holding the shortest straw.

With the problem of fraud correctly identified, a complete solution will be presented that treats all parties to a transaction fairly and most importantly, eliminates all possibility of card transaction fraud.

The Industry Plague



HE PAID THE BILL.

But He Was Sore Because Somebody Else Had Lots of Hack Rides While He Rode Street Cars.

Do you carry a "credit card" issued by a local carriage company? If so, the experience of a well known live stock commission man may serve as a precaution. The "credit cards," which resemble a street car pass, entitle the holder to credit at any and all times. On the 1st of each month the holders of the cards are supposed to settle promptly with the company.

One of these cards was sent to a certain live stock commission man at the yards. He did not care for credit, so he carelessly tossed the card in a waste basket. No further attention was paid to the matter until the 1st of the following month when the company presented a bill for $8. The dealer in live stock could not understand how he could owe the company anything when he had not used his credit card. Upon investigation, it was discovered that someone had picked up the card and used it to an advantage. The stockman paid the bill, and requested the collector to say nothing about it. The victim, in speaking about the matter yesterday, stated that the only thing that made him feel regret was the fact that while he was economizing by riding on street cars someone had been riding in rubber-tire hacks at his expense.

One of the initial premises of credit cards when they were first introduced to the public was that they were safer than carrying cash; the logic being that only the owner of the card could use it. However, this was proved to be untrue from the first reported case of credit card fraud in 1899.

As stick-up men holstered their guns to exploit credit cards, both thieves and victims quickly learned that cards were the opposite of safe. During a hold-up, losses were limited to the cash and valuables on hand, but with a credit or debit card, your entire account and credit balance was available for the taking.

> "That big security fix for credit cards won't stop fraud."
>
> *Wired, September 2015*

> "There is no reason to believe Apple Pay is making you any more or less vulnerable than usual."
>
> Thrillist - Joe McGauley

Despite 120 years of use and dozens of attempts to fraud-proof credit cards, the plague continues nearly unabated, even despite EMV chips and e-wallets such as Apple and Google Pay. The reason for this is that the fundamental concept of payment cards is flawed.

Throughout credit card history, sensitive data has always been transferred between buyer and seller, a practice that still continues today since merchants must present consumer data to the payment networks in order to get paid. So long as this continues, fraud will plague the payments industry because as long as a reward is possible, thieves will find a way to obtain it.

Card security measures have merely stopped the modern equivalent of amateur pick-pockets but since annual credit card fraud accounts for over $30 billion, the industry today faces a more formidable and talented thief. With a reward this large, credit card fraud has become an industry in and of itself, consisting of numerous competing, well structured, well educated and well funded criminal organizations who no longer target consumers directly. Evidence over the last dozen years has shown that the targets of credit card theft are the merchants.

Identification of the Problem

Problem solving theory first requires identification of the cause of the problem under investigation. Focusing on anything other than the root issue of the problem results merely in a treatment of its effects; which of course, assures that the problem will persist indefinum.

The elephant in the room when discussing credit card security is the very thing credit cards represent, —the identification of a consumer and the ability to access their money. In other words, the problem with credits cards is credit cards. This is why after 120 plus years, the problem of credit card fraud is unresolved and why every so-called *enhancement* has merely been a treatment. However, the most recent attempt at eliminating fraud, the EMV chip, actually made matters worse for consumers.

The EMV Non-Solution

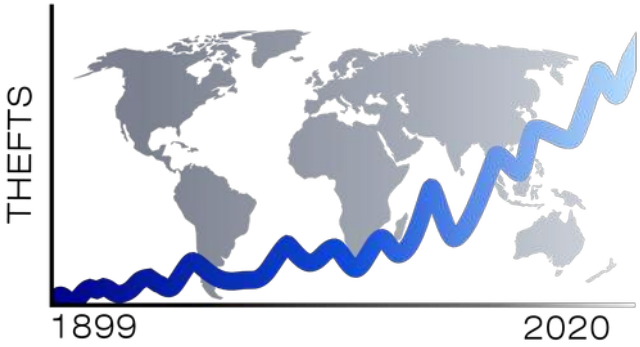
Contrary to its design and what consumers have been told, the EMV chip has not made credit and debit cards any safer –in fact, it has only added *insult to injury*, as the saying goes. Previous to chipped cards, consumer data was confined to the magnetic strip on the back, which was very limited to the amount of consumer data it could hold, which in hindsight was a good thing. It was both hoped and claimed that adding more data to credit cards would help merchants and card issuers positively identify the true card holder by cross-referencing that data with other stored consumer information. The validity of this statement of course depends upon the quality and quantity of the stored data as well as the algorithms employed.

While it is true that the EMV has helped issuers identify fraud after it has occurred, it has done almost nothing to prevent it. The fraud continues and with improved means of identifying it, merchants are being hung out to dry when banks recall fraudulent transactions. This is not to say of course, that fraudulent transactions should stand, it merely illustrates how the EMV is not a solution and actually hurts merchants. However, they are not the most injured by the EMV chip.

Previous to chipped cards, consumer data was confined to the amount that could fit within the magnetic strip, whereas compromised cards now give away a great deal more than just a credit card number. Just as credit cards exposed consumers to greater potential losses over cash, the EMV likewise exposes a great deal more than the old stripped cards. But unlike stripped cards, criminals can scan an EMV chip when in proximity or stolen using bypass cloning.

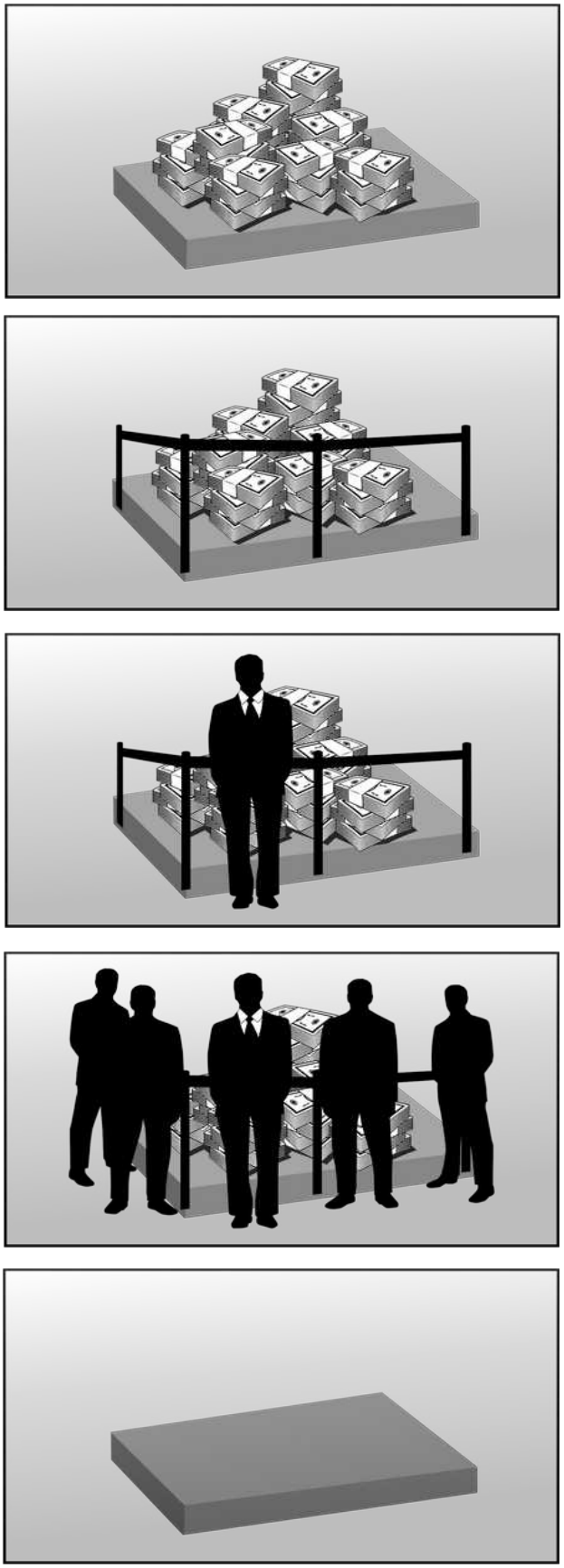
The evolution of credit cards and their lack of security began with their invention; akin to placing a consumer's assets in the public square. Once criminals became aware of the easy payday, safeguards were put in place to prevent access but of course, these simple, metaphorical fences were quickly over come.

Trying to ever stay ahead of the thieves, more and more security features were added to credit cards, some more effective than others but the eventual outcome always the same. After every security enhancement, the statistics showed a decrease in theft and the industry was quick to publish its successes. But just as winter follows autumn, the theft wave has always trailed 2-3 years behind the fix –as it always will so long as there is a reward to be had.



Credit card theft 120 year trend.

The obvious solution is to remove the cash from the public square all together, which is to say, to stop using credit cards, but this is not likely to happen.



Rethinking the Card

With the advent of e-wallets and similar technology, the danger of actually loosing a card through negligence or theft is greatly diminished, thereby frustrating thieves and causing them to focus their efforts elsewhere –on the merchants and the transaction.

The vast majority of card theft happens at the merchant level or in other words, during the hand-off and storage of sensitive data. Similar to the futile efforts to secure credit cards discussed above, PCI Compliance is losing strategy that will never be solved for the reasons already discussed. The only satisfactory action should be to just remove the data out of the merchants hands.

No matter the strength or layers of encryption, the barrier will eventually be breached if the reward is significant enough. Credit card fraud losses in 2019 rose close to 30 billion, certainly a sufficiently significant amount for thieves to keep hacking away at barriers.

Whether we're talking about security policies, data packet encryption or fire-walls, a potential reward is always just inside the shell; a temptation that is too great for some to resist.

An overwhelming number of data breaches suggest insider involvement on some level. This can take the form of stolen passwords and keys to back doors programmed into the software, but cracking the oyster shell doesn't always require hacking skills. Card numbers can be harvested by an employee simply by taking a picture of the card, swiping it on their own pocket terminal connected to their phone or even old-school tactics like writing down the number.

This potential risk is what motivated the creation of PCI Compliance by the Security Standards Council, which like the security measures of the cards, has grown exponentially complex, since its inception, creating burdens on merchants in terms of both time and money to reduce their liability, a liability merchants would rather not have at all. So long as a pearl exists, it will always be in danger.

Therefore, the only viable solution is conceptually very simple; remove the pearl. However, such a solution must still be able to function within the existing payment ecosystem without adding complexity or disrupting habits.

The World XPay solution changes the way cards work without changing current merchant or consumer be-havior. The oyster is still processed, but no longer contains a pearl.

A Consumer-Centric Model

Merchant's currently are responsible for the security of their customer's cards, which represent a portion of their credit and liquid assets; a very heavy responsibility most merchants are simply unaware of just how massive that responsibility is. Merchants dislike the position they have been placed in, that of being required to engage in data security in addition to their preferred focus, that of selling stuff. Anyone who is forced into doing anything will not perform well. The situation would be comical if it wasn't so serious.

Consumers abhor the thought of having to carry something as dangerous as a credit card in their wallet, especially a chipped card that contains even more sensitive information.

Merchants abhor having to be the fraud police and being the man-in-the-middle who ultimately incurs losses when fraud does occur.

Lenders abhor incurring losses due to, as they see it, the casual handling of their cards by consumers, and merchants mindlessly processing any card that is presented to them.

Government and industry councils mandate ever demanding policies that over-burden merchants and adds to their liability; policies that in the end, tend to only favor the lenders.

World XPay's patent-pending solution reverses the payment process, placing the consumer in control of the transaction not the merchant. Merchants never come in contact with consumer data, not even the consumer's name if they so choose. This relieves the merchant of being the man-in-the-middle and allows consumers to work directly with the payment networks. During a transaction, the merchant simply provides the sale data and then waits for the result of the transaction, while the consumer selects the payment method. This consumer-centric system serendipitously provides the consumer with increased privacy, since the merchant is no longer relying information to and from the consumer's bank –a strange and awkward process when you stop and think about it.

Any problems with a person's credit or accounts, should be a private matter between that person and their banker. With the consumer now running the show, if they have a declined card, they are notified privately, not the merchant. If they so choose, they may select a different card or cancel the transaction all together. All the merchant will know is that the transaction was canceled.

The World XPay Ecosystem

Any attempt to improve the payment card industry must be able to accommodate the existing frontier of both cards and standards of processing. Anything too bold, requiring habit changes, no matter how great the improvement, will not be embraced by the consumer or merchant.

The public-facing technology of the World XPay platform conforms and seamlessly merges with the current habits of both consumers and merchants. And even though World XPay is an iron-walled, closed system, access points are securely designed such that, they cannot compromise the integrity of the platform. This is accomplished, not by strong encryption, but through strategic design, such that, in the event of a breach, there is no reward for the effort.

Hardware

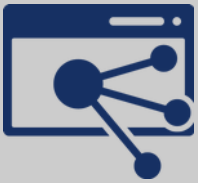
No proprietary hardware is required for merchants or consumers. Merchants can access the XPay Network using a standard tablet or a custom integration with their point of sale.

Apps

The World XPay consumer app is a free download available in the major app stores. Merchants require the official XPay Merchant App.

Ecommerce

Integration with XPay is extremely easy for online merchants, requiring only the addition of a *Pay with XPay* button at their checkout .



Public API

Developers can integrate World XPay into their projects and platforms using a very simple and intuitive API.

Open Bank Platform

The World XPay platform conforms to the Open Bank Project standards, making integration with bank partners easy and inexpensive.

All New Rails

The entire World XPay network is all new from the ground up. At no time does traffic touch the old, congested, proprietary, credit card rails.

From the Merchant Perspective

Preventing transaction fraud is not enough to protect merchants from charge backs. A large portion of charge back related fraud stems from the premise that the merchant processed a payment when they shouldn't have and therefore should absorb the loss. The current system places the burden of policing thieves solely on the backs of merchants, a duty they are neither adequately trained for nor have the required tools and technology to effectively do it. The only tools at the disposal of the merchant is the POS or terminal, which are supposed to validate a card. However, when this technology fails to identify a compromised card, the fault is still placed on the merchant since at the end of the day, funds are withdrawn from their account to compensate the lender and consumer. The current system compensates or protects everyone involved in the fraudulent transaction except the merchant. A consumer-centric system resolves this problem very effectively.

Elimination of Charge backs

The old method of processing placed the merchant as the gatekeeper, which saddled them with the burden of verifying consumer credentials. Because of this, merchants were held responsible for all fraudulent activity under the assumption that it resulted from their derelict of duty; an assumption that is both untrue and unfair. By removing the merchant from the transaction, they are relieved of all liability surrounding the sale and the consumer's payment method.

Return Fraud Protection

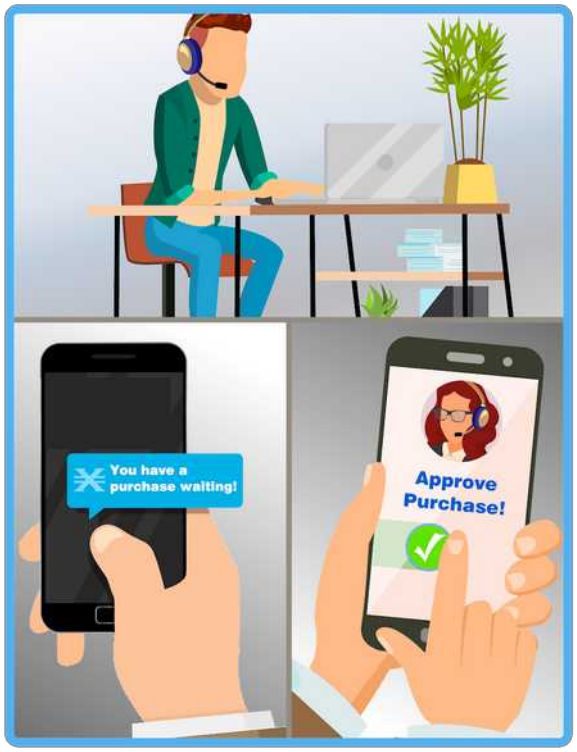
Merchants are hurt regularly from fraudulent returns and refunds. This is because they do not always have the ability to positively identify and link the purchaser with returner, this is especially true with ecommerce sales. When the transaction process is reversed and made to be consumer-centric, the consumer instigates and confirms the transaction, not the merchant. The merchant merely presented the consumer with an offer. The consumer then, must initiate and approve the return from the same device that made the purchase. In such a scenario, a merchant could decline the return without fear of a chargeback; again because the merchant did not initiate the transaction and is therefore blameless.

Simple PCI Requirements

Since the merchant is no longer participating in the mechanics of the transaction, there is no reason they should require PCI Certification; never at any time do they come in contact with a consumer's sensitive data. A major PCI certification firm confirmed this to be true and further stated that if they were to certify a merchant who uses World XPay, the certification would consist of only two questions.

Phone Sales

It's incredulous to think in this technological age we still read credit card numbers over the phone. Since phone lines are not secure, this is not much different than making a purchase on a website without an SSL certificate (a secure connection). Then of course there is the problem of employees keeping a secret record of card numbers and/or eaves-droppers on both ends of the phone doing the same. In the current global economy, phone sales and order taking has become very important for merchants. The phone sale introduces a special set of issues for merchants, in addition to the security ones mentioned above. This is especially true for merchants who have never taken phone orders but are now forced to in order to remain in business.



In a consumer-centric payment model, the security problems surrounding a phone sale vanish. As illustrated to the left, when a consumer calls in an order, the merchant pushes a sales offer to the consumer containing the details of the order and total due.

The consumer, being in control of the transaction, accepts the offer and approves the sale; no sensitive information is ever exchanged.

Once the transaction is complete, both the consumer and merchant receive a notification of the result. As previously mentioned, if there is a problem with the consumer's payment method, only the consumer is notified of the issue, whereupon they may select a different card from their wallet or simply cancel the order.

Push Sale Technology

Within a consumer-centric model, marketers will discover many new marketing opportunities, such as a push sale. Since the consumer initiates the transaction, a sale can occur anywhere. Instead of designing advertising to lead consumers down a sales funnel toward an hopeful sale, the sale can happen at the first contact, in real-time.

All marketing and advertising effectively become a point of sale.

Powerful messaging can be immediately rewarded with a sale; no more analyzing click-throughs or wondering how effective your last mail drop was.

Purchase Codes can be placed anywhere, creating greater convenience for customers and the ability to capture the impulse purchase which is nearly non-existent with database and direct marketing.

Purchase Codes can be any size. Placing them in emails will allow consumers to purchase without even clicking. Print advertising can now be just as interactive as electronic media, making a powerful sales letter even more powerful.

Whereas the goal of traditional advertising is to keep one's brand top-of-mind in order to capitalize on a future sale, the sale can now happen in real-time the moment advertising is viewed, whether it be television, print, email, text, business cards, or outdoor

FROM THE CONSUMER PERSPECTIVE

The heart of a consumer-centric model must contain processes and ultimately, technology that allows the consumer to be in control. While such a model could be implemented without it, mobile technology makes the process more accessible, convenient, and faster. The World XPay App, currently developed for the iOS and Android platforms, is a free download available in the United States and Canada with a global roll out currently in development.

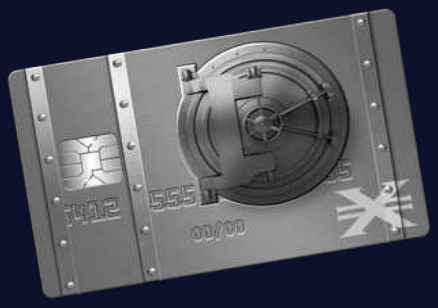
Fraud-Proof Transactions

The World XPay App contains a card wallet similar to other payment apps, but that is where the similarity ends.

Once a card is entered into the wallet, no sensitive data of any kind remains on the device, not even the consumer's name. The sales interaction takes place without any sensitive data being exchanged between merchant and consumer, and can therefore not be stolen or intercepted.

Touchless

Touchless payments have quickly become a requirement for may consumers and merchants. On the XPay platform, there are no touch points during a transaction, proximity is not even required. A payment can be just as easily processed when the consumer is standing at the checkout counter or on the other side of the planet.

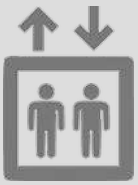


Purchase Privacy

During a transaction, communication is unidirectional, from merchant to consumer. In addition, since no personally identifiable data is stored on the consumer's device, it cannot be transferred to a merchant. While merchants receive transaction reporting, such reports are devoid of all consumer data, unless the consumer expressly agreed to provide it to the merchant. This provides unprecedented privacy in today's economy where prying eyes seem to be everywhere.

The core of what is known today as World XChange was discovered in 2017 at Platinum Age Merchant Services, when the *fraud-proof credit card processing* concept was first realized, coded and proven. World XChange was officially incorporated in 2019 with World XPay as the company's flagship technology, which generated immediate excitement within the limited scope in which it was showcased.

World XChange is more than just a new payment platform, it embodies a whole new paradigm in which to manage and facilitate core financial processes. At the core of our business philosophy is the belief that if a solution to a problem cannot be found, it is because we are asking the wrong question. It was this kind of thinking that enabled us to develop a platform that is more private (or completely private if utilizing our entire platform) and more secure than any platform in history. The ripple effect from this new technology has created a whole new world of benefits and opportunities for every participant in a transaction, beginning with marketing and the ease (and safety through touch-less technology) of the purchase, down to protecting and growing income and savings.



ELEVATOR STATEMENT

World XPay is the world's first and only guaranteed transaction fraud-proof payment platform. Our patent-pending technology also provides a layer of privacy, never before equaled in card processing and shifts the locus of control from the merchant to the consumer.

Our technology simplifies the entire payment process, making transactions easier and faster. World XPay changes how cards work on the existing payment networks, which not only revolutionizes the payment industry but sales, marketing, and advertising as well. Our powerful and very disruptive Push Sale Technology changes the entire sales landscape, heralding the end of sales funnels, abandoned carts and even the click-through statistic.

MISSION STATEMENT

We exist to pioneer and build laissez-faire business solutions through thin technologies that provide and support critical processes with minimal interference.

World XChange is a privately held corporation, guided by very experienced hands from the financial, payments, banking, technology, business, marketing and sales disciplines; each one a seasoned life experiencer, undeceived by the waves of unprofitable and unsustainable ideology so prevalent in popular culture today.

World XChange Inc.
PO Box 7492
Loveland, Colorado 80537

http://world-xchange.com
hello@world-xchange.com
833-473-XPAY (9729)

"We foresee a bright future for the world; one where fraud and wide-spread deception no longer go rewarded and unchecked."