Multi-Factor Verification

Applying the Power of Community to Fight Digital Payment Fraud

Mike Kontorovich, Mark Chazan & Ian Mirels

With digitalisation transforming the ways organisations transact, new opportunities are emerging for criminals to engage in digital identity theft and fraud. The challenge for organisations when it comes to addressing this risk is:

How can your organisation verify the legitimacy of a counterparty to a transaction in a fully digital environment?

A new approach is needed that will enable you to establish counterparty legitimacy in digital transactions.

We believe that addressing this challenge requires all organisations to come together and share crucial information for the common good by harnessing the power of decentralised information.

In this whitepaper, we outline our unique approach to solving this challenge. We call it: Multi-Factor Verification.

SECTION 1: Digitalisation and Decentralised Information

The digital revolution has barely begun.

Yet, even at this relatively early stage, it is no exaggeration to state that digitalisation has comprehensively transformed the modes by which humanity lives, works and interacts. For better or worse, the digital revolution is ushering in a radical paradigm shift in the functioning of societies.

Perhaps digitalisation's greatest impact is in transforming the ways we acquire and use information.

Before our very eyes, people are becoming less dependent on centralised information sources as the basis for knowledge and decision-making. Thanks to the emergence of the internet, new networks of people are continuously emerging that facilitate the sharing of information as never before.

In this new networked world, there is increasing scepticism towards centralised information, or the 'Single Source of Truth.' No longer are people willing to believe, without questioning, information that disseminates from official or authoritative hierarchies, such as governments and 'experts.'

Thanks to networks, people are acquiring information from a multitude of decentralised sources. Some of this information is accurate. Much of it is not. But, through a process of aggregation over time, many believe decentralised information has the potential to uplift knowledge levels in ways that centralised information simply cannot.

This transition is having profound implications. Each time we learn something through reading Wikipedia, decide which route to drive using Waze, or opt to verify ledgers using blockchain, we are making decisions based on decentralised information systems.

> ***"Decentralised systems…benefit from being able to aggregate the knowledge and ideas of the many…Instead of relying on a central decision-maker to determine in his or her wisdom how a system should be run, decentralised systems rely on the collected wisdom of the masses. To the extent that these masses have better knowledge about relevant information, they should be able to come to more informed decisions than a single authority figure".***

William Magnuson
Associate Professor of Law, Texas A&M University
Blockchain Democracy: Technology, Law and the Rule of the Crowd

However, it would be wrong to think that decentralised information is totally displacing the role of centralised information. The two approaches are not mutually exclusive.

Circumstances still exist in which people look to hierarchies for information. The COVID-19 pandemic is a recent case in point. Likewise, decentralised information sources can also be problematic. The spread of 'fake news' through social media comes to mind.

It is our view that optimal outcomes are achieved when centralised and decentralised approaches are in alignment. When information from centralised sources align with information from decentralised sources, it provides far greater confidence that the information is legitimate.

In some respects, alignment between the centralised and the decentralised is not entirely new. After all, we live in a liberal democracy in which government decisions (centralised) derive their legitimacy from a broad network of citizens (decentralised) via the ballot box.

However, what is new is our ability to extend this approach to an unlimited range of new applications, thanks to digitalisation.

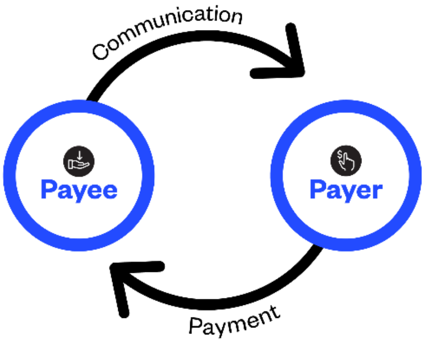
It's our mission is to help organisations fight fraud by aligning information from centralised and decentralised sources, so organisations know whether the information in their possession about their counterparties is legitimate. This is necessary, as in the world of digital transactions, Information Asymmetry exists which makes knowing the legitimacy of your counterparty a significant challenge.

SECTION 2: The Challenge of Information Asymmetry

As discussed above, digitalisation opens up new opportunities for acquiring decentralised information. When centralised and decentralised information align, it offers the potential for conferring a strong degree of legitimacy on that information.

However, when it comes to any type of economic transaction, a problem arises when one party has access to more, or better, information than the other. This is known as Information Asymmetry and it erodes trust between parties, causes friction in interactions, and ultimately may lead to market failures[1].

In the case of digital payments, particularly Electronic Funds Transfers (EFT), the challenge of Information Asymmetry between the payer and payee is exacerbated due to a number of factors connected to digitalisation. Prior to a payer transferring funds to a payee, the payer is reliant on communications relayed from the payee. This is known as the EFT Payment Cycle.



However, that communications relayed from the payee may be inaccurate, either through deliberate manipulation or error. As a result, a state of Information Asymmetry exists between the parties. There are two types of factors that lead to Information Asymmetry: Payment factors and Communications factors.

2.1. Payment Factors

PAYER RELIANCE ON LEGACY PAYMENT INFRASTRUCTURE

Many of the digital payments technologies in existence are built on platforms designed for a pre-digital world. This is particularly the case with EFT systems, which were originally designed for processing analogue payments, such as cheques.

Prior to digitalisation, bank tellers would manually verify all the details on a cheque before processing it. They would verify that the Account Name on a cheque aligned with the BSB and Account Number. Whilst this was time-consuming, the advantage was that both parties to the transaction had confidence in the legitimacy of the counterparty.

[1] Ross, Sean, *The Theory of Asymmetric Information in Economics*, https://www.investopedia.com/ask/answers/042415/what-theory-asymmetric-information-economics.asp, 2020.

The development of EFT payments has been superimposed onto this pre-digital system. However, now that bank tellers are no longer verifying payments, there is no ability to ensure alignment between an Account Name and the BSB or Account Number.

As a result, a payer does not have full visibility over whether they are actually processing EFT payments to the legitimate payee.

PAYER RELIANCE ON ENCRYPTION TO FACILITATE DIGITAL PAYMENT

Digital payments would not be possible without advances in cryptography. Encrypting data is an essential prerequisite for enabling secure and private transfers. Without it, there would be no online banking or EFT payments.

However, whilst encryption allows for security and privacy, it also allows fraudsters to hide behind a veil of anonymity.[2]

Encryption can result in a lack of transparency when processing digital payments. A payer has no way of being certain that a payee isn't abusing the capabilities of cryptography to disguise their legitimate identity.

2.2. Communication Factors

PAYER UNAWARE OF PUBLICLY ACCESSIBLE INFORMATION

As organisations embrace digitalisation, they inevitably extend their network perimeter and integrate additional applications into their environments. This enables the accumulation and telemetry of more data than ever. However, it also makes securing data more challenging.

Data leakage from vulnerable networks, applications and the APIs that connect them, means that fraudsters can conduct extensive reconnaissance, or 'Social Engineering,' in advance of committing any crime. They can acquire information about their prospective victims either directly through hacking, or by sourcing that information via other means, such as the dark web.

The result of extensive data leakage is that an attacker has access to extensive information about a payer and are therefore able to conduct attacks that are highly targeted and effective. By contrast, a payer has access to limited information that confers legitimacy on the payee with whom they are interacting when processing digital payments.

PAYER UNAWARE OF GEOGRAPHIC LOCATION OF PAYEE

Prior to digitalisation, criminal activities usually required the criminal to be in close geographic proximity to the scene of the crime. After all, a bank robber had to physically attend the bank he intended to rob.

[2] May, Timothy, *The Crypto Anarchist Manifesto*, https://groups.csail.mit.edu/mac/classes/6.805/articles/crypto/cypherpunks/may-crypto-manifesto.html, 1988.

In a digital world, geographic location ceases to be any barrier to attacks.

For example, studies show that Business Email Compromise (BEC) attacks are overwhelming carried out by criminal syndicates based in Africa. This occurs despite most targets being in advanced economies, such as Australia.

Technologies that enable email spoofing and the masking of IP addresses, allow fraudsters to hide their true physical location. A payer can never know for certain the final destination of any funds they transfer electronically, putting them at a significant disadvantage in knowing whether the payee is legitimate.

PAYER UNAWARE OF FRAUD RISK DUE TO AUTOMATION

Prior to digitalisation, carrying out fraud was a slow and mostly manual process. Even attempting to defraud one target required a significant investment of time and effort.

With digitalisation, automation now allows fraudsters to carry-out mass defrauding attempts.

One example of this is MalSpam, in which bulk email servers, usually used for spam, are engaged in the distribution of large quantities of emails containing malware. This 'carpet bombing' approach only requires a very small percentage of targets to be deceived in order for the fraud to succeed. Once a target erroneously runs the malware, fraudsters can gain access to their confidential data in order to manipulate emails and files.

In many cases the payer is totally unaware that the malware has been installed in their systems.

PAYER UNAWARE OF FRAUD RISK DUE TO NEW TOOLS

Prior to digitalisation, the range of tools available to fraudsters was limited. A plethora of new online tools, many of which are free, allow fraudsters to create fakes that, to the untrained eye, are indistinguishable from the genuine article.

Such tools allow a fraudster to generate fake emails, corporate logos, even entire websites. These are all designed to deceive a payer into believing that they are transacting with a legitimate payee. The latest tools even allow for the creation of 'Deep Fakes,' which synthetically recreate the voice of a party to a transaction in order to compromise call-back verification procedures.

Such tools result in a situation in which a payer can never know with confidence that their counterparty is legitimate.

As a result of all these factors, an acute Information Asymmetry challenge exists when it comes to digital payments.

Studies have demonstrated that Information Asymmetry in other domains can be addressed using Internet-based reputation mechanisms.[3] Typically, this involves the aggregation of decentralised data in order to verify the reputation of the parties to an economic transaction.

[3] Tabarrok, Alex, and Cowen, Tyler, *The End of Asymmetric Information?* https://www.cato-unbound.org/2015/04/06/alex-tabarrok-tyler-cowen/end-asymmetric-information, 2015.

Review websites, such as TripAdvisor, or e-commerce sites, such as Amazon, all make use of decentralised data from multiple sources to overcome the challenge of Information Asymmetry. A buyer can know the legitimacy of a seller before entering into an economic transaction based on the information aggregated for multiple other buyers.

We believe that the principles used to address the challenge of Information Asymmetry in other domains, particularly Internet-based reputation mechanisms, can also be applied to the fight against digital fraud.

SECTION 3: Our Approach: Multi-Factor Verification

Our goal is to mitigate the risks of fraud that exist when processing EFT payments.

To achieve this, we have developed a tripartite approach to verifying the legitimacy of parties to a digital transaction: Multi-Factor Verification.

At its core, Multi-Factor Verification is based on two elements:

1. The power of decentralised information.
2. Aligning decentralised information with centralised information.

Until now, payers have been forced to rely solely on centralised information when processing digital transactions. This presents a significant problem. Centralised information is based upon a 'Single Source of Truth' which can be compromised by nefarious actors. While there is still value in centralised information, it allows for a state of Information Asymmetry to emerge with the payee and is thus incapable of offering the level of verification that is required to confer legitimacy on a counterparty to a digital transaction.

Multi-Factor Verification does not envisage abandoning centralised information. Rather, we argue that whenever decentralised information can align with centralised information, it provides far greater legitimacy to payers, and helps close the Information Asymmetry gap.

Centralised information can come in two forms:

1. Enterprise: This can be in the form of communications with the counterparty, or enterprise, you are transacting with. It can include emails and call-backs. The problem with this type of information is that they are vulnerable to breaches. Emails are regularly compromised (witness the rise in BEC attacks), whilst new technologies allow for 'Deep Fakes' that synthetically manipulate voices in call-backs.

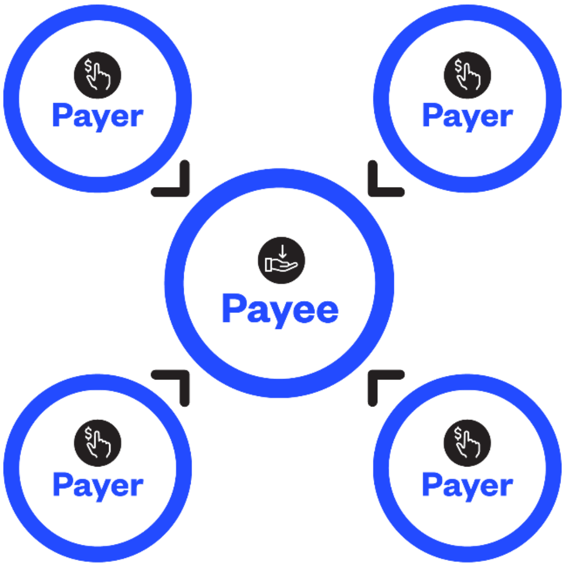
2. Authority: This is usually based on official records, such as the ASIC register. The problem with such information is that malicious actors are known to use tools to manipulate such records, creating highly realistic forgeries.

Thus, while both forms of centralised information have their value, both can be vulnerable to sophisticated fraudsters. Both are based on a 'Single Source of Truth' that means they do not offer the level of verification or legitimacy that payers require in the fight against fraud.

Introducing a new way to verify: Community

For the first time, we introduce a decentralised information approach into the digital payment verification process.

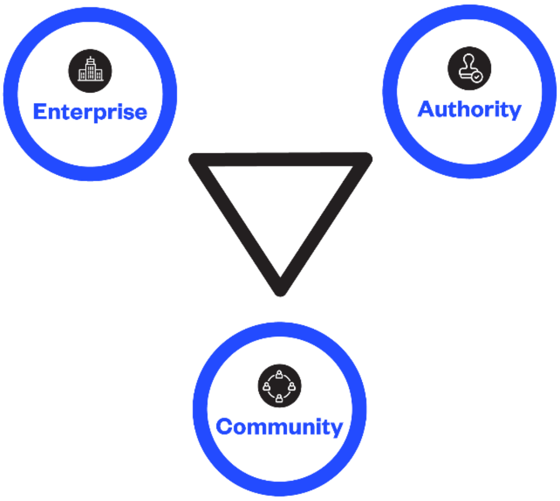
Our unique platform aggregates information from a community comprising nearly 2 million Australian organisations into a comprehensive database. This allows us to verify that other organisations have transacted independently with the same counterparty using matching banking data. This independent proof-of-payment allows a payer to confer a strong degree of legitimacy on a payee.



The strength of this approach is that it cannot be easily compromised. The fact that a counterparty has received EFT payments from multiple, independent payers in the past, without incident, makes this approach unique and robust. Any nefarious actor would need to manipulate many multiple datapoints to undermine the veracity of the database. And given that the database is continuously expanding with more participants joining the community, it ensures it becomes more robust over time.

We are not suggesting that centralised information is now redundant. However, it becomes increasingly valuable when it can be verified against decentralised information. fraudtech solutions built around this methodology help payers determine the veracity of centralised information in ways that were not possible before.

In summary, Multi-Factor Verification is about aligning information from the Enterprise, the Authority and the Community. When this occurs, it provides an unprecedentedly strong degree of legitimacy in the veracity of the counterparty to a digital transaction.



This level of veracity addresses the many Information Asymmetry challenges payers face in the world of EFT payments. It provides payers with the confidence they need to ensure they are transferring funds to the legitimate recipient. When payers are armed with trusted, verifiable information, the ability of fraudsters to hide their identities and deceive payers is fatally undermined.

By using the power of decentralised information and enabling payers to align it against centralised information, we can provide a new way to address the growing threat of fraud that is strengthening the ability of organisations to process digital payments.

Conclusion

We aim to address the growing risk of fraud in the world of digital payments.

Whilst digitalisation opens up many new possibilities, it also opens up new risks. Digitalisation allows for a state of Information Asymmetry to emerge between parties to a digital transaction. By aggregating decentralised information from the Community and aligning this with centralised information from the Enterprise and Authorities, an approach we call Multi-Factor Verification, it is possible to establish the legitimacy of your counterparty when transacting digitally.

This allows organisations to fully embrace digital payments without being exposed to the growing risk of fraud.

We believe the approach of using decentralised information in this way has many real-world applications beyond digital payments. We hope this whitepaper acts as a catalyst for others seeking to address the challenges posed by digitalisation and Information Asymmetry in other domains.

About the Authors

Mike Kontorovich
With over 35 years' experience in IT, Mike has extensive experience as a software architect and technologist. Over the course of his career, he has co-founded four start-ups with a strong focus on the rapidly emerging fintech sector. In his capacity as CEO and CTO at eftsure, Mike has spearheaded the development and enhancement of the functionality of the eftsure platform. His unique perspectives are enabling organisations to solve the growing problem of EFT payments fraud.

Mark Chazan
Co-founder and Chief Risk Officer of eftsure, Mark is an engineer, accountant and technologist with 30 years of experience working across a range of solutions from engineering automation software to mobile financial apps. Mark has had numerous local and international patents granted in the financial technology industry.

Ian Mirels
Ian is a Founder of eftsure. As a Chartered Accountant and a member of The Institute of Chartered Accountants in Australia, Ian has a deep understanding of accounting practices, corporate governance, and internal controls. Throughout a career spanning South Africa, USA and Australia, including 7 years with Ernst & Young, his focus was on the burgeoning IT industry, giving him unique perspectives on financial software applications.

For more information visit https://get.eftsure.com.au