



IS BANK-BASED DIGITAL IDENTITY THE MISSING LINK IN SOLVING PAYMENT FRAUD?

HOW DIGITAL IDENTITY PROVIDES THE MISSING WEAPON IN THE FIGHT AGAINST PAYMENT FRAUD, AND HOW BANKS, REGULATORS AND PAYMENT SCHEMES CAN READILY ENABLE THIS.



CONTENTS

Executive summary	3-4
The fraud problem	5-7
Fraud prevention measures – current state of play	8
The online safety challenge	9
Digital identity, supported by banks	10-11
Managing multiple attack vectors online	12
Integrating digital identity with payments will strengthen protections	13-18
Conclusion	19

EXECUTIVE SUMMARY:

Fraud is now classified as a national security threat. Along with computer misuse (used to obtain identity data to carry out fraud), fraud now accounts for **50% of all crimes**. According to UK Finance, **criminals stole £580m in the first six months of 2023**.

Payments are increasingly compromised.

In addition to the emotional distress consumers face when they are compromised with fraud, the cost of fraud is priced into the business models of major companies. Against the context of a cost of living crisis, combined with the need to control inflation, tools that can cut fraud and thus offer better pricing are valuable to companies in their efforts to deliver more value to hard-pressed families.

UK regulators have introduced three key fraud-prevention measures:

- **Strong Customer Authentication (SCA) to validate online payments**
- **Confirmation of Payee (CoP) to validate recipient names**
- **Rule changes for banks to shift the cost of Authorised Push Payment (APP) fraud away from the customer and split it equally between sending and receiving banks**

The payment systems operator Pay.UK is currently developing an additional tool, Enhanced Fraud Data (EFD) Messaging, a means to share account activity and payment information between banks to cut fraud.

Today, most of the approaches for securing payments used in the UK assume the corporate or payment provider initiating the payment has checked identity as part of onboarding. However, this is not always the case and leaves gaps that fraudsters can exploit. For example, the BACS Direct Debit scheme rules require identity to be checked and account ownership to be confirmed upon set up of a direct debit.

When a direct debit mandate is signed digitally, as many onboarding and payment processes now are, this requires the validation of the identity to be digital at the point of set up – a digital identity to secure the payment and confirm the person making it, is really who they say they are and that they were present at the point the mandate was signed. This is often not done.



Payments fraud is particularly severe given the increase in payments now made online at ecommerce stores and major corporates. Corporates do not yet have a ready means to confirm digital identity at the point of customer onboarding, interaction, and payment initiation, and are highly vulnerable to compromise through account takeover and stolen or synthetic identities.

This paper explains how bank-based digital identity, which has been proven in Europe to achieve very large reductions in fraud, can provide the missing link in the end-to-end payments chain to control fraud. This is achieved by checking the identity of an account, or at the point of initiation of the digital payment – a process that will become mandatory in the EU in the next few years as governments roll out digital identity wallets under new legislation which large merchants must support.

Already in Norway, where banks support their corporates with digital identity (BankID), fraud has been reduced from **1% to 0.00042% of payment transactions**. Itsme in Belgium reports a 27% reduction in one year of reported phishing attacks.

We also set out how a bank-based digital identity certified under the UK government's digital identity trust framework provides a ready solution to the fraud problem in the UK, and the actions regulators and market infrastructures can take to banish the fraudsters from our shores.

Bank-based digital identity also improves the consumer experience by reducing friction in the journey. Moreover, it is inclusive, supporting all consumers with online bank accounts. Consumers share their data with consent, rather than type it, and businesses have the assurance of knowing it is correct, also saving the need to correct the data, which in itself is a growing business overhead.

OneID[®] is the UK's first FCA-regulated, government-certified digital identity provider supported by leading banks. It was founded to enable banks to offer a bank-based identity service to their corporate and personal customers and is already proven and operational in the UK. As a B Corp, OneID[®] has set out its social purpose to achieve online safety and reduce fraud through the use of better digital identity tools.

THE FRAUD PROBLEM

The financial impact of fraud is borne by individuals, businesses, government (taxpayers) and banks (shareholders). UK Finance publishes bi-annual statistics on the scale of two key categories of fraud:

- “Authorised” fraud - Authorised Push Payment (APP) fraud is a growing problem in today’s online services (£485m lost in 2022).
- “Unauthorised” fraud, consisting mainly of card fraud and remote banking fraud:
 - Card Not Present (CNP) fraud is an ongoing problem (£556m lost in 2022).
 - Remote banking fraud cost the industry £163m in 2022, mainly through unauthorised access to online banking.

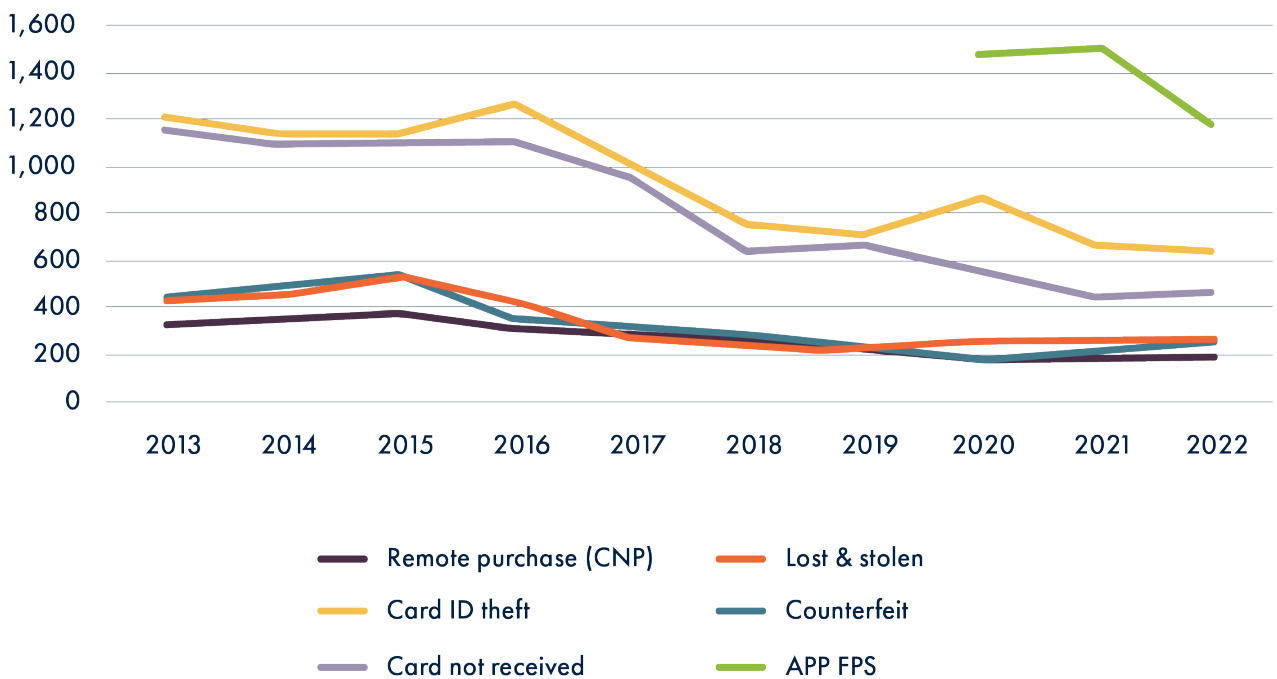
The cost to banks in just these two categories of payment fraud exceeds £1.2bn and that excludes abuses in Direct Debit and other payment methods.



IMPACT PER CASE

Per case, APP fraud average transaction values are about 6-9x CNP card losses (£1,150 vs. £178 average loss per case in 2022). The impact of each APP case is therefore much bigger than card fraud, and the customer has less protection.

AVG LOSS PER CASE



The average loss for card ID theft (fraudster obtains a card in someone else’s name) and card not received (fraudster intercepts the victim’s card) are also higher than CNP, at £630 and £452 respectively. Preventing identity theft, therefore, has a bigger impact per case.

WHO PAYS THE COST OF FRAUD?

The cost of APP fraud is borne by customers (34% of APP fraud in 2022) and banks (66%), whereas CNP fraud cost is borne by banks and retailers (depending on liability rules).

The APP cost balance will tip further towards the banks when the Payment Systems Regulator (PSR) rule changes come into effect in April; as an illustration, using 2022 data at a 95% reimbursement rate, bank costs would increase by £109m overall. Sending banks' costs reduce by £70m, but receiving banks have a new cost of £179m. Impact for each bank will depend on whether they are a net receiver or sender of fraudulent transactions. Net receivers of fraud will have significant new costs to manage.

2023 cost (2022 data)	£m	If 95% returned	Change
total lost to fraud	376.1	376.1	
% returned	66%	95%	
total returned to customer	248.6	357.3	
total lost (customers)	127.5	18.8	-108.7
total lost (sending banks)	248.6	178.6	-70.0
total lost (receiving banks)	0	178.6	178.6
total lost (banks)	248.6	357.3	108.7

More significantly, proceeds of fraud are used to fund other serious crimes including terrorism, drug trafficking, human trafficking, modern slavery and child abuse.

Shifting the cost of fraud away from the customer is a good thing, but this just increases the cost to the banking sector. More needs to be done to shift liability to where fraud originates.

FRAUD PREVENTION MEASURES – CURRENT STATE OF PLAY

The banking and payments industries and regulators have introduced a number of measures to reduce fraud over the last few years:

● Strong Customer Authentication (SCA)

as part of the 2nd Payment Services Directive (PSD2). Uses multiple authenticators from 'something you have' (e.g., mobile device, card reader), 'something you are' (e.g., biometrics) and 'something you know' (e.g., PIN, passcode) to make it harder for fraudsters to take over accounts or use stolen data to make payments.

Mandated by FCA, applies to online banking, card payments, account-to-account payments (but not direct debit or other 'merchant-initiated payments').

● Confirmation of Payee (CoP)

was built in response to rising APP fraud, and returns the name of the payee to the payer, who then makes the decision to make the payment or not. This has had some impact on fraud reduction and reducing errors in mistyped sort and account numbers, but fraudsters can coach victims through the warning screens and customers don't always heed the warnings.

Mandated by PSR. Applies to Faster Payments and CHAPS.

2024 will bring new measures that add to SCA and CoP:

● Rule changes for Faster Payments

A further change to combat the impact of APP fraud,

is that the current voluntary code for customer reimbursement is becoming a mandatory [AF1] rule change for Faster Payments from April 2024, when the customer will be refunded in most cases, unless negligence can be proven.

In October 2024, a rule will be introduced that will split the cost of fraud 50/50 across sending and receiving banks. The intention here is to put more focus on 'who is banking the fraudster?'. Banks are responding by increasing inbound transaction monitoring, but there is a challenge to meet FPS timescales for crediting the beneficiary account.

Mandated by PSR. Applies to Faster Payments.

● Enhanced Fraud Data (EFD)

Banks will share extra data between themselves about both accounts and payment purpose during payment processing (without customer knowledge). This is the last line of defence before the money is lost to the fraudster.

Provided by Pay.UK, initial focus is Faster Payments but can be used across other schemes.

SCA, CoP, FPS rules and EFD all play their part. But they exist within the banking and payments domain; we need additional tools that let us extend measures into the online services domain where the fraud originates. Fraud needs a continuously evolving response to keep up with the technology that is deployed to defraud victims and where commercial transactions are increasingly taking place – online - and we argue that part of that response is digital identity.

THE ONLINE SAFETY CHALLENGE

Impersonation fraud, purchase scams and many other fraud types, are enabled by unverified accounts and spoofing over insecure channels. The Online Safety Act (OSA) will compel online service providers to remove illegal content and use age and identity verification to reduce risks of online harms, including fraud. Ofcom is currently consulting on the act's implementation, which is due at the end of 2024.

In our submission to Ofcom, we have advised that unverified users should not be allowed to trade or offer goods or services for sale; fraudsters take advantage of anonymous accounts to impersonate others, use synthetic ID names and disappear without delivering goods paid for.

Requiring a verified account to trade should be standard practice, e.g. in the card scheme model, a merchant 'acquirer' provides a merchant account and is responsible for fraud carried out by its merchants. A similar approach could be used for platforms that want to capture value from trading; they should be liable for the behaviour of their users. Verification brings with it accountability.

Platforms that enable trading should be required to educate and inform their users to only message each other via the platform, and not to move onto unsafe channels where contact details can be spoofed (e.g. phone, email, SMS).

Payments should also be made via payment methods that have been enabled by the platform, that are safe and that provide customer protection (which could be underwritten by the platform). Clear communications for users that they have protection for trades on-platform, and no protection if they move off of it, will reduce fraud. Ebay took this approach, successfully, when they acquired PayPal.

Verifying accounts brings accountability to them and enables enforcement if account owners carry out illegal activity. It also prevents fraudsters from just opening new accounts whenever their unverified accounts are closed down; there is a higher cost for them to create new verified accounts, and it is much harder to do.





DIGITAL IDENTITY, SUPPORTED BY BANKS

Digital identity is an essential tool in the toolbox of fraud prevention measures, enabled by the Department of Science, Innovation and Technology (DSIT), and the Data Protection and Digital Information (DPDI) bill that will soon become UK law.

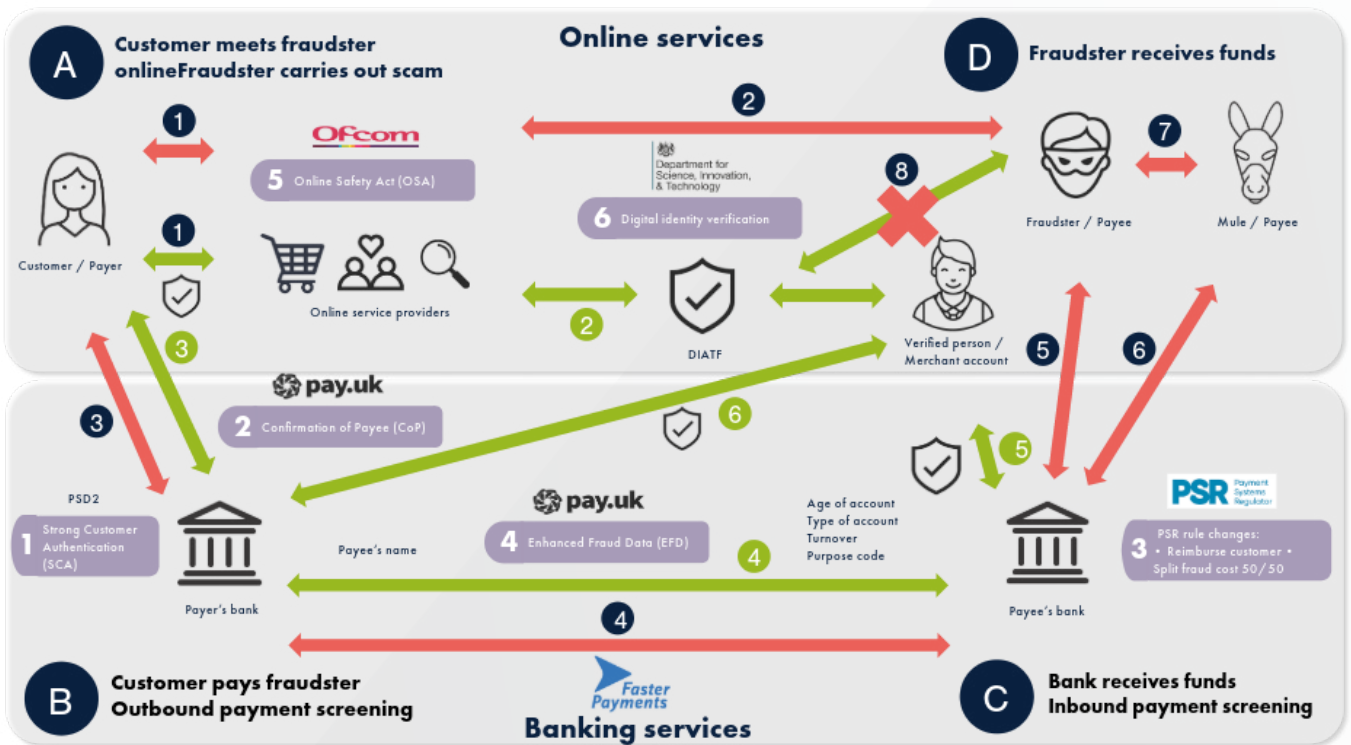
Using a bank-based digital ID will enable closer integration of online services with UK banks and payment schemes, providing more data for fraud prevention into the 'payment rails' and fraud decisioning engines. Making greater use of previously verified identity in systems and processes will provide fraud defences that we lack today.

The DSIT identity framework, the Digital Identity and Attributes Trust Framework (DIATF), also enables certified identity providers to simply and securely verify people online. Whilst SCA, CoP and EFD all give focus within the banking domain and shifting 'downstream' with the PSR rule changes, this helps with getting to where the fraudster has access to bank accounts.

However, much more focus is needed 'upstream', in the online platforms where the fraudsters are actually targeting their victims. A combination of DSIT-certified identity and Ofcom's enforcement of OSA laws will enable weak points in the payment initiation chain to be addressed; turning the red lines into secure green ones where the identity of both parties is known (diagram below), cutting off the fraudster and money mules from the process.

Using a strong digital identity will discourage fraudsters as they don't like revealing their true ID, and money mules can be given additional warnings not to share their accounts.

A bank-based digital identity enables a low-friction identity check to be done as part of adding a new beneficiary, for instance. Currently the beneficiary is entirely passive in the set-up flow (other than giving the sender bank details over insecure channels); having an active step will strengthen the process without adding much friction.



MANAGING MULTIPLE ATTACK VECTORS ONLINE

Digital identity helps ensure:

SIMPLE, SECURE ORDERING AND CERTAINTY ON DELIVERY



Digital identity enables a simple and secure guest checkout, or 'onboard and pay' user experience that can be completed in a few steps, and less than 10 seconds. The retailer has

certainty that the person is a real person, the right person, and that the address is that which is held by the bank for them. This massively reduces the risk of shipping goods to an incorrect address, so it saves the retailer the cost of lost goods. Once the goods arrive at the address, the customer can prove who they are via an easy, quick process such as a QR code, e.g., if the goods need age verification (as per remote alcohol sale legislation).

SECURE ACCESS WITH MUTUAL AUTHENTICATION, E.G. CALL CENTRE



Digital identity can be linked to a corporate identifier to prove that someone is an employee of that organisation, reducing impersonation fraud. An individual calling from a bank or government department can prove that they work thereby presenting a signed digital credential that can be verified.

Fraudsters will not be able to obtain the same credentials, so anything they present will appear as invalid. The customer can, in return, share their digital credentials to prove who they are digitally, saving the call centre valuable time since they no longer need to ask security questions. This has the added benefit of enabling the education of customers never to answer questions that give away personal information (a typical fraud attack vector to steal ID information).

The sharing of verifiable credentials enables a strong, quick mutual authentication of both parties.

PREVENTING ACCOUNT TAKEOVER

A bank-based digital identity can help to prevent account takeover fraud by enabling Strong Customer Authentication to be used to protect the account as it extends the use of SCA to other use cases – any online journey.

The 'authenticators' that protect an account (typically weak usernames, passwords or SMS processes) can be strengthened to bank-based security. This stops the fraudsters from accessing telco accounts, for instance, as they cannot bypass someone else's SCA. Readily available personal data and social engineering of call centre staff, for instance, enables SIM swap attacks; these would be reduced if SCA protected the telco account.



INTEGRATING DIGITAL IDENTITY WITH PAYMENTS WILL STRENGTHEN PROTECTIONS

UK payment schemes – 3 examples of ID improvements

A bank-based digital identity can enable better customer journeys and reduce fraud



DIGITAL IDENTITY AND DIRECT DEBITS

The BACS scheme rules require any direct debit 'service user' to carry out KYC on the mandate-signer, and to prove that they own the account that is being used – but this rule is mostly not being adhered to. There is no customer KYC, and typically a 'mod check' is carried out to check that the sort code and account are a valid combination, but no ownership check is done.

Using a bank-based digital identity gives both a KYC check to a high level of confidence, and verifies the account ownership, with the additional bonus of removing payment failures from mis-typed account data.

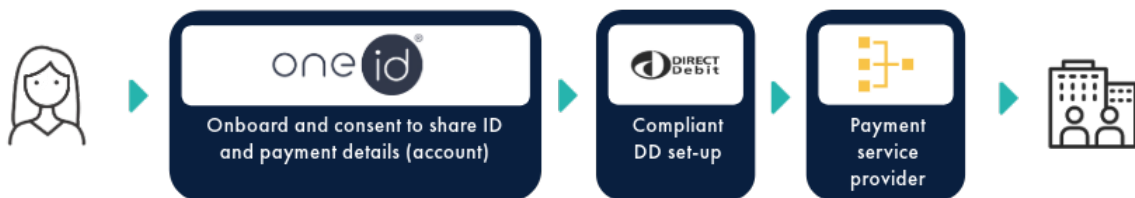
1 Direct Debit – current journey



Current problems	❌	❌	❌	❌	❌
Manual data entry (name, address, DOB)	Manual data entry (sort code, acct. no)	KYC check not done*	DD fraud DD failures DDIC	DD fraud DD failures cost £1.4bn DDIC cost £250m	
<ul style="list-style-type: none"> inconvenient prone to error 	<ul style="list-style-type: none"> fraudster can use stolen details 				

*BACS DD scheme rules require a KYC and account ownership check; this is mostly not done today

1 Direct Debit – OneID journey



New journey	✅	✅	✅	✅
Data via API	Identity check	Reduced DD fraud	Reduced DD fraud	
<ul style="list-style-type: none"> security convenience improved data quality 	<ul style="list-style-type: none"> complies with scheme rules fraudsters unable to authenticate 	<ul style="list-style-type: none"> Reduced DD failures Reduced DDIC cost 	<ul style="list-style-type: none"> Reduced DD failures Reduced DDIC cost 	

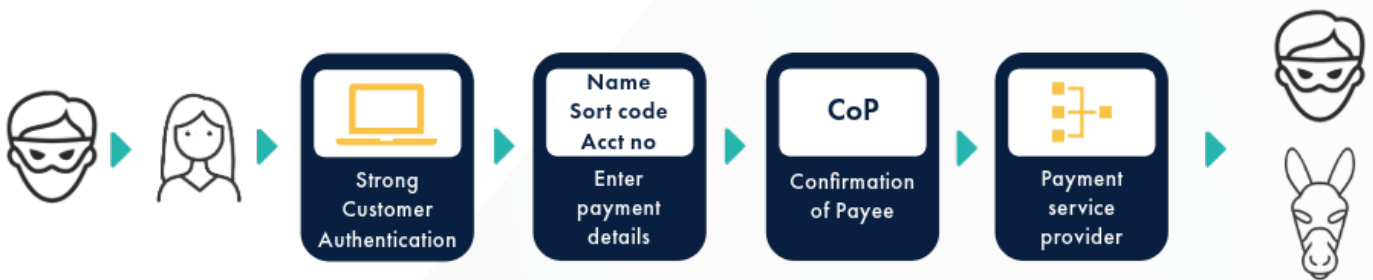
DIGITAL IDENTITY AND COP (FOR FASTER PAYMENTS)

Confirmation of Payee is a type of identity solution; sharing one attribute (the payee’s name) with the payer where they confirm that the response (full match, partial match or no match) is what they are expecting. This relies on the payer making the fraud decision, and also the manual bank transfer process involves the sharing of bank account details, so can be improved from a privacy perspective.

Using a digital identity solution in addition to CoP provides additional benefits:

- Better privacy – data is shared with consent, and only to parties that need it; this could be just the banks, protecting the customer data from being seen by either end party.
- More data – attributes such as name, date of birth, address, email and phone number could be shared with consent; this enables better risk scoring to be done by the banks.
- ‘Upstream’ fraud checks – fraud checks can be done at the online platform level, or by the sending bank before a payment is initiated; this avoids payment costs and holding payments or tipping off of fraudsters.

2 Faster Payments (P2P/B2C manual payment, with Confirmation of Payee)



Current problems



Fraudster scams victim



SCA
• only identifies sender



Manual data entry
(name, sort code, acct. no) • fraudster uses scam or mule account



Customer ignores



Customer stops



APP fraud



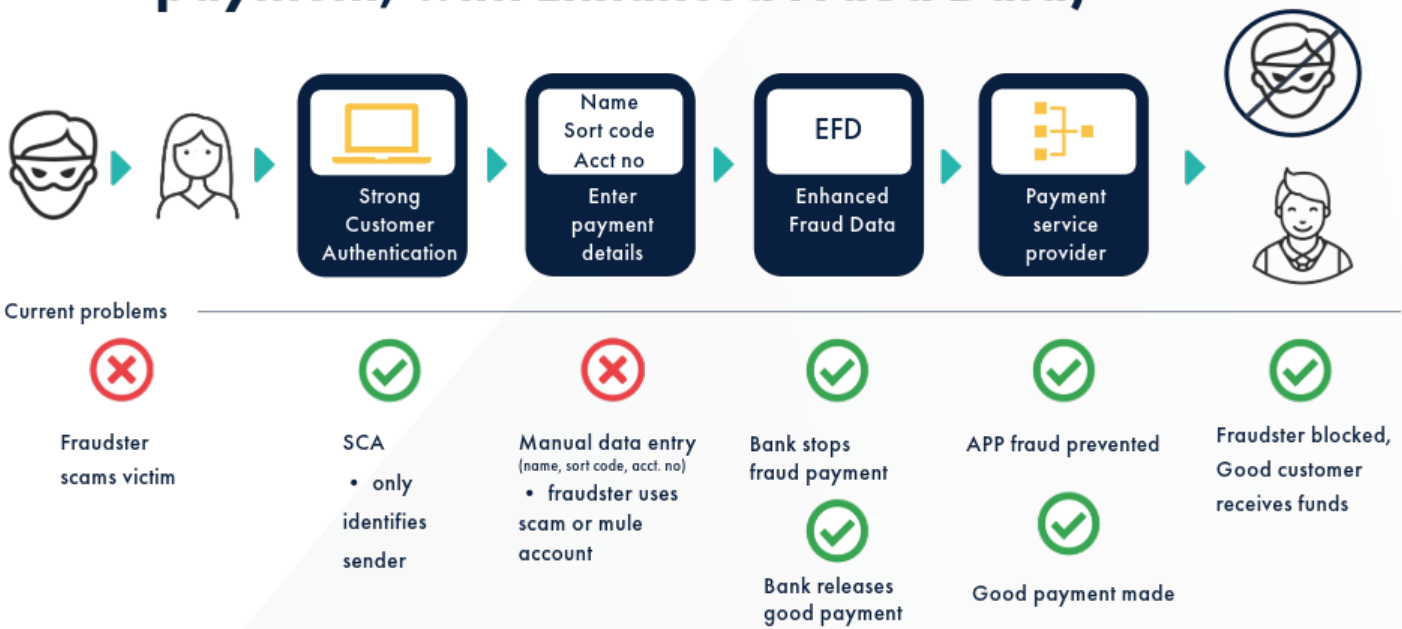
Fraudster obtains funds

ID AND EFD (FOR FASTER PAYMENTS)

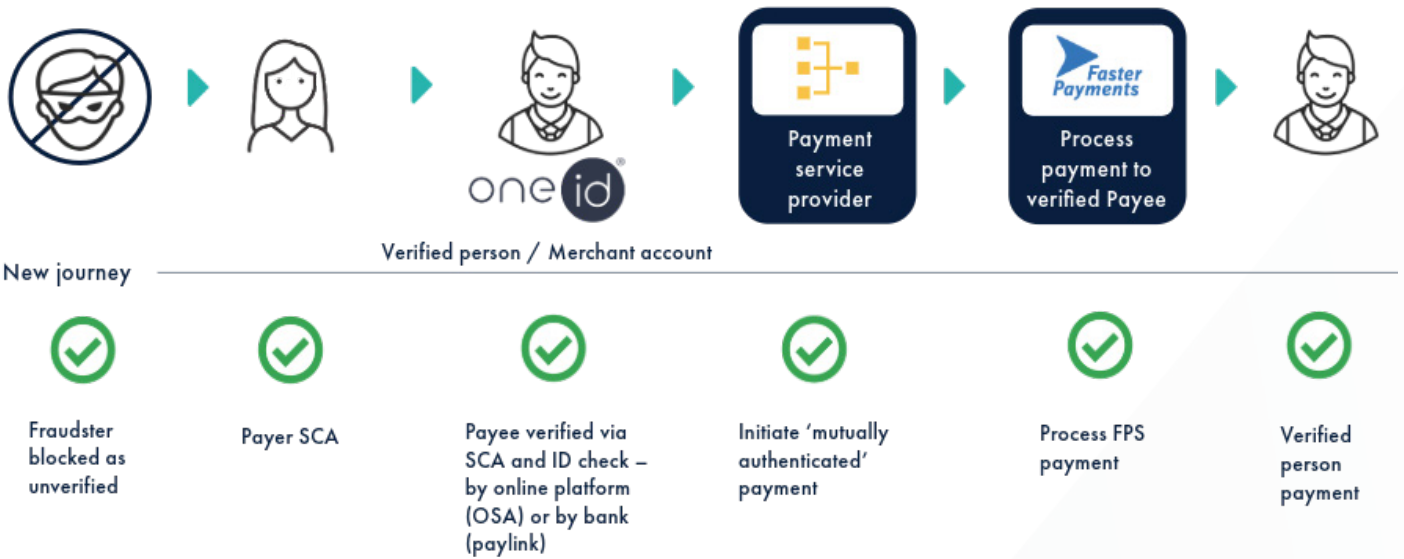
In the identity space, we now have a global open standard for sharing ID data, with the OpenID Foundation's [OpenID Connect](#). There is an extension specification for sharing Know Your Data (KYD) metadata too; [OpenID Connect for Identity Assurance](#).

These global standards enable certified ID providers to supply ID data in a standard way into payment schemes. This standard data can then be used in payment messages such as EFD, or ISO20022 messages (if fields were available). Linking digital ID into EFD would connect the online and banking domains to give banks greater visibility of where the transaction is originating from, and real-time checks of who the parties are, along with consent to use the data under GDPR.

2 Faster Payments (P2P/B2C manual payment, with Enhanced Fraud Data)



2 Faster Payments (P2P/B2C manual payment, with mutual authentication via eID)



DIGITAL IDENTITY AND CARD PAYMENTS

If banks could provide real-time card details via API, a bank-based ID check (via SCA) could also retrieve card details that could then be sent into the acquirer processing; this would enable industry and merchant cost reduction from no longer needing 3DS, or PCI-DSS over time – merchants would no longer need to store any card data, increasing security. Expired cards would also no longer be a problem, fixing a current pain point for corporates (failed payments) and customers who need to update details.

Stolen card details and CNP fraud would become a thing of the past.



3 Card – current journey

Worst case – cards generally work well, but CNP is still high & some legacy problems remain

Hacked data Risk of GDPR fine
Cost of PCI-DSS Expired cards
Unauthorised payment
Lost track of CoF



Current problems

- 

Manual data entry
(name, address, DOB)
(username, password)

 - inconvenient
 - prone to error
- 

Manual data entry
(PAN, expiry, CVV)

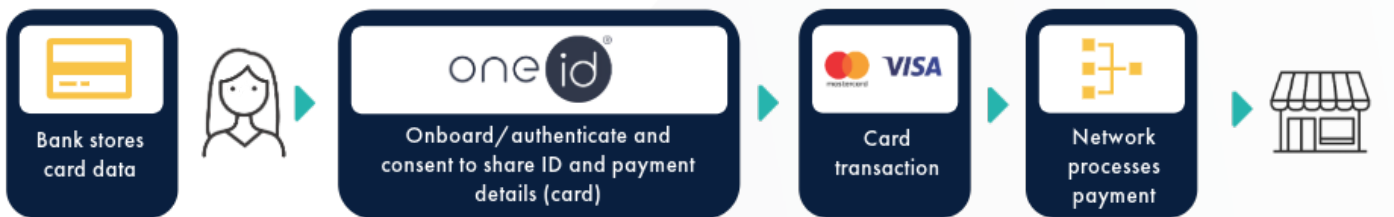
 - fraudster can use stolen details
- 

3DS problems


 - poorly implemented
 - inconvenient
 - adds cost
- 


Chargebacks for fraud
- 

3 Card API (future?) – OneID journey




New journey


- 


Protected data
Updated cards
Tokenisation
Virtual cards
- 

ID check & data via API

 - convenience
 - improved data quality
 - fraudsters unable to authenticate
- 

Card data via API

 - reduced need to store card data
- 

Reduced need for 3DS
- 

No PCI-DSS
Chargeback protection from 1st party fraud

CONCLUSION

Bank-verified digital identity confirms the identity of the person at the point they make the payment. It is a quick and simple solution which supports SCA at the point of onboarding, set up of direct debit mandate and payment to merchants.

Bank-verified identity services are ubiquitous in many countries around Europe. Their impact on reducing fraud is profound and the benefits to banks, corporates and consumers is tangible. The UK has a bank-verified ID service built, government-certified and operational, accompanied by a set of identity of scheme rules to support it. OneID[®] was founded to enable banks to provide a bank verified ID service to all their customers. It is available to them now.

OneID[®] recommends that the following six actions be taken by the relevant parties to help prevent fraud and enable the benefits of digital identity to be realised:

1. Regulators to support the UK in the move to digital identity as a benefit to consumers and the economy, mandating digital ID for online safety and enabling it for use in payment rails.
2. Trade bodies to convene banks to support current digital identity initiatives, aiming for a critical mass of adoption.
3. Banks to develop and extend their use of bank-based digital identity, taking this service to their corporate customers.
4. Government to accelerate the adoption of digital identity by merchants and corporates, through new enabling legislation e.g. replacing the need for a physical identity to be shown when a certified digital identity could be used, such as age verification in a supermarket, or higher value corporate and digital payments.
5. Payment schemes to accelerate their efforts to embed digital identity tokens validating identity at the point of payment initiation into the payment message for Enhanced Fraud Data.
6. Merchants and corporates to strengthen their digital customer onboarding and collaborate on pilots to reduce their fraud using digital identity.

○ About OneID®

OneID® is the only provider of truly digital, real-time identity services that create absolute certainty between a business and a customer, in the fastest, cheapest and safest way.

Our digital ID services use the most advanced counter-fraud measures to help protect banks, businesses and consumers from online identity fraud. By streamlining existing ID processes, including payments, direct debits, onboarding and more, we help businesses reduce operational costs, increase sales and improve customer engagement. As the only UK Identity Service with access to bank-verified data, nearly 50 million UK adults are already set up to use OneID®, for real-time verification.

OneID® is government certified, regulated by the FCA and is a BCorp business.

Headquartered in the UK, we have brought together the best people in Digital Identity, Payments, Banking, Technology and Government to ensure we make the world a safer place.

To learn more visit www.oneid.uk.

Scan to learn more



○ FOR MORE INFORMATION
Contact Rob Kotlarz,
Co-founder and President
rob.kotlarz@oneid.uk

