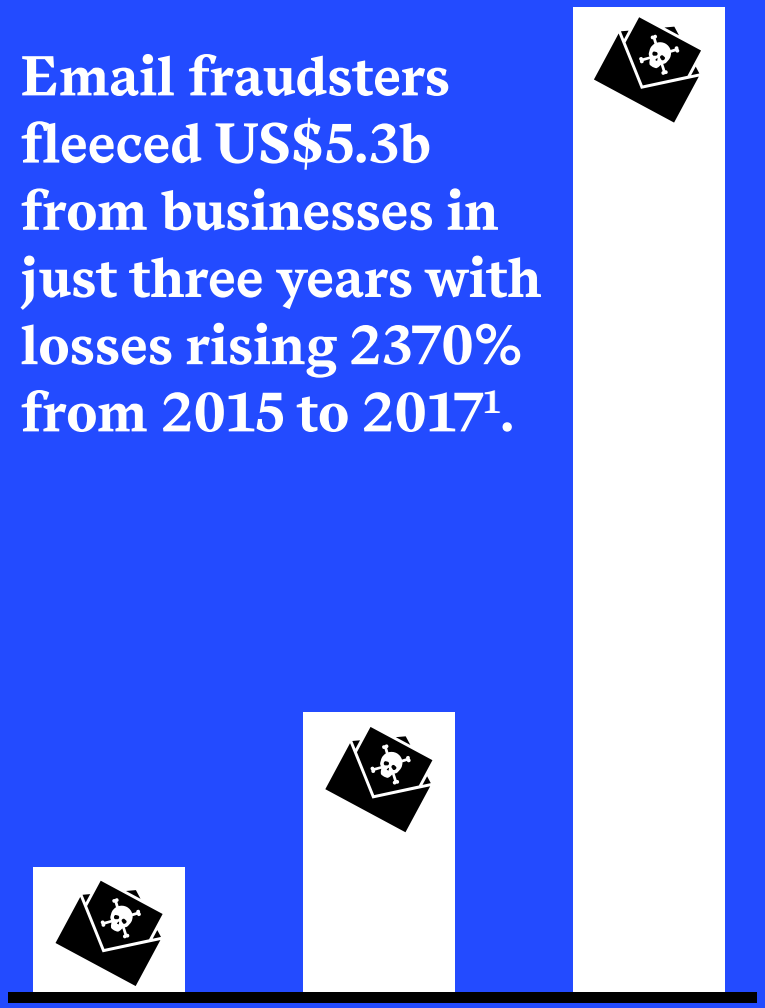
The importance of a correct and up-to-date Vendor Master File

Your first line of defence against fraud and error.

eftsure

Contents

Email fraudsters fleeced US$5.3b from businesses in just three years with losses rising 2370% from 2015 to 2017[1].



1. *FBI Internet Crime Complaint Center, May 2017*

Companies are under attack

How can you fight back?

With fraud rising relentlessly in Australia and cybercriminals casting a wider net, business risks are accelerating. A 2014 PwC survey found that in just two years, 57% of Australian organisations experienced economic crime, 36% of them losing more than $1m[3].

Scammers, swindlers and fraudsters

Today's fraudsters are determined and sophisticated, and even the world's most tech-savvy companies, like Facebook and Google, aren't immune to their schemes. Using fake email addresses and supplier credentials, they lay the groundwork for payment scams, waiting patiently to whisk funds away.

Inside jobs

They also operate from within: in recent years fake invoicing schemes hatched by employees cost Channel Seven $8m and NSW's Botany Bay Council more than $4m. KPMG says[4] that while frauds by professional criminals rose an astonishing 300% from April to September 2016 in Australia, most were carried out by company insiders, with technology playing an increasing role.

Compliance risks

Some suppliers quote fraudulent GST and ABN details to avoid tax, as tradespeople did in the recent Bunnings scam, exposing businesses to compliance risk. The black economy is now a $25b per annum problem, costing taxpayers and the economy. Many scams go undetected.

Plain old human error

More mundanely, people make mistakes. Human error, pure and simple, can lead to significant financial loss through inaccurate or duplicate payments.

How can you protect your business?

The simple answer is better controls. But what's the best way to implement them without slowing your business down? In this eBook, we explore how you can improve digital payments controls and compliance while achieving best practice vendor master file (VMF) management. By validating payees and payments in real time, you can stay ahead of criminals and reduce errors that lead to financial losses.

US$100m

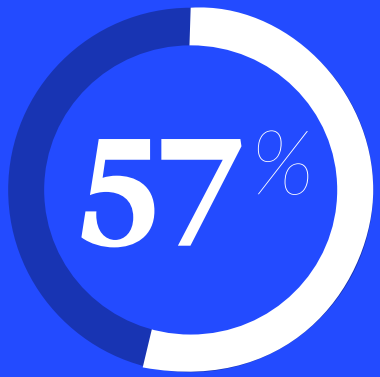
lost by Facebook and Google in an email phishing and payment scam in 2013.

Posing as genuine supplier, the swindler coaxed accounting departments into making wire transfers to a fake supplier account.[2]

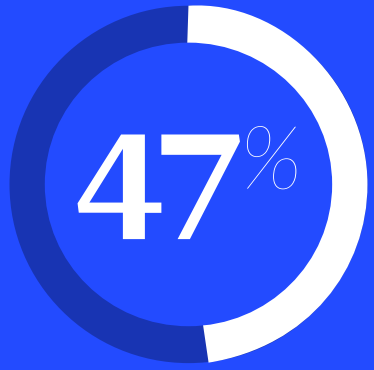
2. *Fortune, 2017*
3. *PwC's 2014 Global Economic Crime Survey: The Australian Story*
4. *KPMG Fraud Barometer, January 2017*

No place for complacency

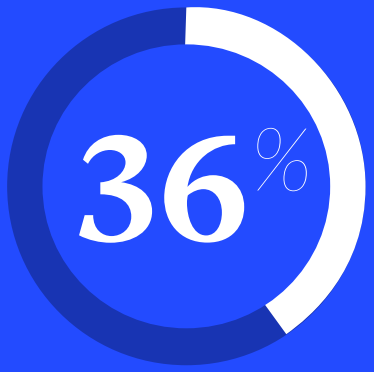
A 2014 PwC survey[5] of Australian organisations found that in the previous 24 months:



EXPERIENCED ECONOMIC CRIME



EXPERIENCED 10+ FRAUD INCIDENTS



LOST $1 MILLION OR MORE

> “eftsure’s [adds] extra strength to our internal control enviroment.”

DUNCAN STEWART
Breakthru People Solutions

5. *PwC’s 2014 Global Economic Crime Survey: The Australian Story*

Why is correct and up-to-date Vendor Master File (VMF) so important?

Your VMF reaches into every part of your business.

It's not called a master file for nothing

A healthy VMF, or supplier database, is critical because the data is used to generate electronic payments and also used in a huge range of business activities. It's fundamental to everything from business-to-business transactions to tax and GTS reporting. And it touches management reports, compliance, purchasing, sales, contracts, sourcing, performance and risk management. So it's vital to keep your VMF clean - and to protect it with sensible data management processes and policy.

Inaccurate VMFs are the norm

Keeping a VMF up to date manually is a time -and labour- intensive task, and many businesses fall short. A recent KPMG study[6] discovered that 20% of vendor details may be inacurrate in a typical VMF, and eftsure's own analysis reveals the number may be as high as 25%.

So what?

The same study showed that a VMF anomaly rate of 20% results in a payments error rate of 1%. For corporations or government organisations making multi-million-dollar payments, this represents a significant and largely avoidable loss. For small to medium enterprises, a cyberattack can be ruinous, putting them out of business for good.

The good news?

Well-maintained and automated, your VMF can be your secret weapon in combatting fraud and error. Used wisely, it can improve governance and compliance reporting and protect your business from risk.

6. KPMG, study details, year, link etc - details to be provided by Ian.

> "Fraud continues to rise relentlessly in Australia"
>
> GARY GILL
> Head of Forensic at KPMG Australia

How clean is your VMF?

Your VMF probably started out clean enough. But it degenerates over time.

Why do errors occur?

There are many reasons why VMFs degenerate. The biggest is human error. It's compounded by many factors - multiple owners, decentralised business operations, shoddy controls and the fast pace of business putting time pressure on workers. The sheer volume of vendors can make it difficult to keep up with changing address or banking details. Fraudsters expertly find and exploit these weaknesses.

What are the consequences?

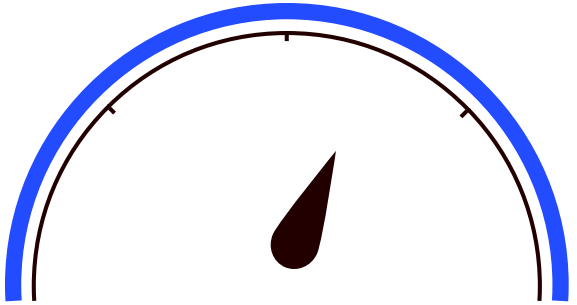
Inaccurate VMFs are implicated in a swathe of payment problems - everything from duplicate or misdirected payments to overpayments and fraud. They can also cause your business to run foul of regulation.

How can you clean up your VMF?

It's hard to guard completely against human error but, as we'll explain later, eliminating manual processes and automating checks on VMF additions and changes can have a big impact. This is particulary important when onboarding new vendors. Fortunately automation solutions are now available to help you.

Large supplier ecosystems with frequently changing details make VMFs notoriously difficult to maintain.

Analysis of a wide range of VMFs reveals up to 25% of vendor details are incorrect, incomplete or duplicated, escalating risk exposure.



Top 4 reasons for inaccurate VMF

1 PEOPLE

- *Human error, insufficient resources and poor communication across multiple departments can lead to data entry mistakes and record duplication.*

2 POLICY

- *Poor controls and processes permit too many people to add or change vendor details.*
- *Data is not properly validated when entered or is incomplete.*
- *Governance is inadequate.*
- *Spend analytics are inaccurate.*

3 SYSTEMS

- *Poor controls and processes permit too many people to add or change vendor details.*

4 VENDOR

- *A complex vendor ecosystem where vendor details change frequently can lead to duplicate and incorrect vendor entries.*
- *Vendors go bankrupt*
- *There are obscure related vendors*

What's best practice?

Managing your VMF should be ongoing and in real time - not something you do once in a while.

Efficient VMF management

The best managed VMFs feature both internal and external controls and processes that are continuously applied to keep VMF data accurate. Where possible, they're automated. This removes the risk of human error and partial checking.

The benefits of external controls

External controls can deliver rich data verification capabilitiees, providing automated checks and balances that stop fraudsters from exploiting trust. By enabling third-party credentialling, you can catch many frauds and errors before a vendor's details are even entered into your systems and before money leaves your company account.

Validation points

There are many validation points you can use. For example, matching account names with account numbers and BSBs is a simple way to catch fraud and error. Banks don't do this for you - software like eftsure's can handle it automatically. Validating ABNs and GST registration verifies that your vendor is legitimate business and genuinely remitting the GST they're charging you. Matching addresses provides certainty that vendor details are accurate.

Get vendors involved

Where possible, allow your vendors to easily maintain their own data by using a third-party verification service, such as eftsure, before entering their data into your systems. By giving vendors ownership, you can improve efficiency and reduce inaccuracies.

BEST PRACTICE CHECKLIST

- Provides continuous, real-time and automated vendor verification.
- Offers independent source of truth for payee data.
- Matches payee name with BSB and account number.
- Prompts for missing data during record creation.
- Helps to identify related vendors (cross-vendor, parent, subsidiary, multiple locations or divisions).
- Refreshes outdated information.
- Deactivates old accounts.
- Provides secure self-serve for vendor updates.
- Supports ICAC and State Audit Office guidelines.
- Functions as a Computer Assisted Audit Technique (CAAT).
- Specifies internal controls and enhances corporate governance.

3 steps to a squeaky clean VMF

Combat payment errors and fraud with this best practice approach.

In the real world, keeping things clean requires ongoing effort. So while cleansing your VMF is an important first step, it's only a stop-gap meaure unless you also commit to keeping it clean.

As a first step, you'll need to validate all vendor data before it enters your systems. Then you'll need to check, verify and correct your data continuously - plus protect it from human error and cyberattacks, such as malware, as records are updated and added.

From a compliance perspective, it's also vital to evaluate how you manage your VMF against key metrics to make sure your approach is the most efficient and low risk.

Step 1 : Clean

Your objective

To transform a reactive VMF with poor controls into one that's clean (for now).

First, scrub your VMF to ensure all vendor data is accurate and comprehensive, removing any duplicate and inactive records.

- *Correct innacurate and outdated data*
- *Add missing data*
- *Eliminate duplicate and inactive vendors*

TIPS

- *For organisations with a small number of vendors, this is often the most critical step.*
- *Understanding the links between vendors can go a long way, helping you to remove duplicates caused by cross-vendors, partents, subsidiaries and multiple locations.*
- *Beefing up the data in your vendor records can improve governance and compliance reporting, so make sure to add any missing data points, such as ABNs.*
- *Using VMF automation software and the cloud, you can enable real-time verification and outsource some of this work to experts, allowing you to achieve best practice with less risk.*

Step 2 : Stabilise

Your objective

To make your VMF more automated so it stays clean and consistent and becomes a tactical tool.

Keeping your VMF clean requires housekeepping. Establish processes to keep existing data tidy and complete and to minimise human error, preventing inaccurate data from creeping in.

- *Continuous error correction*
- *Data entry checks and controls*
- *Roles and permissions*

TIPS

- *For organisations with a modest number of vendors, this step is the sweet spot.*
- *Centralising ownership of your VMF is vital. That way you can standardise who can alter it and how it is managed; for example, naming conventions, adding/changing workflows and profile completion.*
- *Don't forget to establish an approval process for adds and changes - by providing an audit trail you can also improve accountability.*
- *Software can help you automate this step by building checks into data entry to make sure your team uses consistent naming conventions and completes each profile, protecting your VMF against error and fraud.*
- *Using VMF automation software and the cloud, you can enable real-time verification and outsource some of this work to experts, allowing you to achieve best practice with less risk.*

Step 3 : Optimise

Your objective

To make your VMF more self-maintaining so it becomes a powerful strategic asset that helps you comply with regulation, manage risk and protect against fraud.

Are you getting it right? Use automation to improve compliance and governance. Plus review, evaluate and improve how you manage your VMF to ensure compliance down the track.

- *Regulatory compliance and fraud protection*
- *Vendor validation at onboarding and self-service*
- *Spend management*

TIPS

- *For organisations with a large number of vendors, this step is crucial to create forward-looking and strategic financial systems.*
- *By collaborating with vendors as you onboard them and by providing self-service for vendors updates, you can improve the accuracy of your VMF.*
- *Don't forget to build VMF maintainance into your governance framework so it becomes an ongoing task, not a one-off activity.*
- *Ensure dual authorisation controls are in place to safeguard internal changes.*
- *Using VMF automation software and the cloud, you can enable real-time verification and outsource some of this work to experts, allowing you to achieve best practice with less risk.*

On fraud's front line

Defrauded, phished and scammed, these companies turned to eftsure to help detect fraud and prevent future losses. Now their VMF management is best practice.

All payments are verified to make sure they're going to the correct accounts. Real-time checks preserve the integrity of the VMF over time. And a full audit trial of alerts and reporting helps managers to stay vigilant to stay vigilant against future attacks.

Company A: Defrauded

37 cases of fraud over two years resulted in losses of $1.2m

eftsure verified all accounts payable transactions and the VMF against our database to reveal phantom vendors, fake invoices, duplicate invoices and fake credit notes. All exploited flaws in confirming payee account information at the point of payment.

Company B: Phished

A phishing scam cost the company 457,288 in fake invoices

A fake hotspot on free airport WiFi directed a finance manager to a spoofed web page that captured his email login credentials. The fraudster replaced emailed invoices from new vendors with fraudulent invoices from a false email address and sent them to Accounts Department with a request to update bank details.

Company C: Scammed

Employees colluded to steal $128,706 over nine months.

The fraud used false invoices from an approved supplier. The gang changed the supplier's account number and BSB, leaving the payee name, and colluded to authorise the payments. Later, they changed the supplier details back to the correct information to allow legitimate payments and audit.

eftsure's report uncovered almost 5,000 anomalies in vendor data in Company C's master file.

Summary Anomaly Report 5 April 2017

Risk	Report Section	Item	No. of Records with Anomaly	Report Anomaly %	eftsure Benchmark %
Critical	AI	Incorrect bank account number	730	4%	1%
High	B	Similar bank account name but different account number	1,095	6%	3%
Caution	CD	Duplicate supplier records	1,278	7%	9%
Caution	D	Mismatch with supplier's official bank account name	535	3%	3%
Caution	ES	Supplier's bank account name mismatch in other customer's VMFs	560	3%	1%
Caution	FI	Invalid ABN	150	1%	6%
Caution	GA	ABN mismatch with ASIC registered company name	191	1%	1%
High	HI	Incorrect GST status	208	1%	1%
Total			**4,747**	**26%**	**25%**
Total number of records checked			**18,256**		

Need help keeping fraud and error at bay?

Talk to us about improving your internal controls

eftsure helps minimise business risk with three user-friendly products collectively known as the 'Known your Payee' (KYP) Solution.

About eftsure

We're a software company that helps organisations know their payees and achieve best practice vendor onboarding, payment controls and VMF management. Our crowd-sourced cloud solution helps you bring your internal control enviornment into the digital age we now transact in.

We save you time and money, and make you more efficient by helping you authenticate vendor's details as you onboard them. We also verify your payees, clean your VMF and keep it clean by providing real-time continuous prevention and detection of fraud and errors in the payment process.

3 powerful products to protect your payments

We have three products that work together to tighten your digital payment controls. Our three products - *VENDORsure*, *PAYsure* amd *COMPLIsure* - work together and make your Accounts Department more efficient, compliant and alert to fraud and error. Their key capabilities are outlined in the diagram.

Know Your Payee Solution

VENDORsure
VENDOR CONTROLS

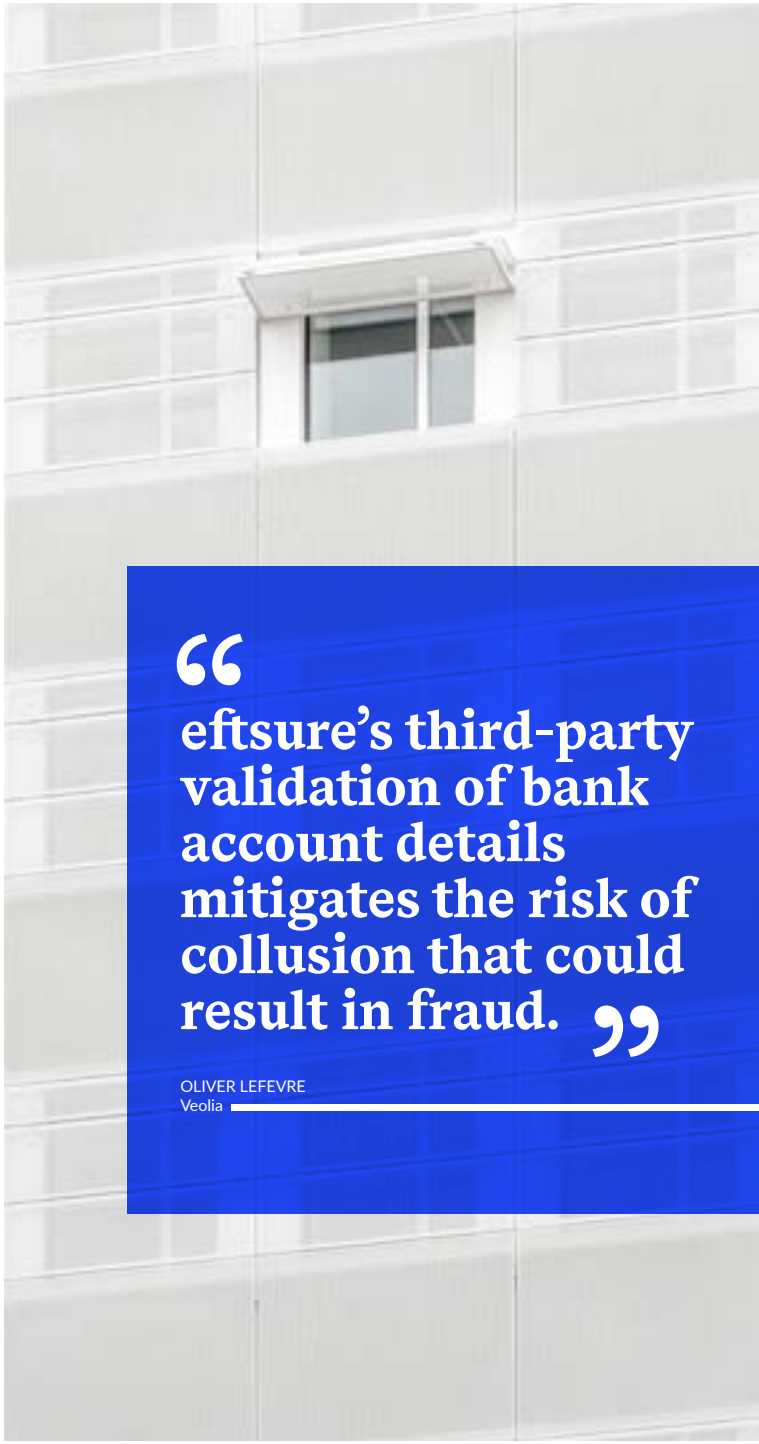
- VMF cleansing (risk scorecard)
- Vendor onboarding
- Vendor data collection, verification + maintenance
- Outdated date refresh
- Continuous monitoring + alerts

PAYsure
PAYMENT CONTROLS

- Payee name matching to account numbers and BSBs
- Out-of-range paayment alert
- Duplicate payment alerts
- Employee payroll authentication

COMPLIsure
COMPLIANCE CHECK

- ABN real-time status checks
- GST status reporting
- Taxable payments reporting (3-way match)



> "eftsure's third-party validation of bank account details mitigates the risk of collusion that could result in fraud."

OLIVER LEFEVRE
Veolia

How eftsure protects your business

We help you ensure you're dealing with who you think you are. 'Know your Payee'.

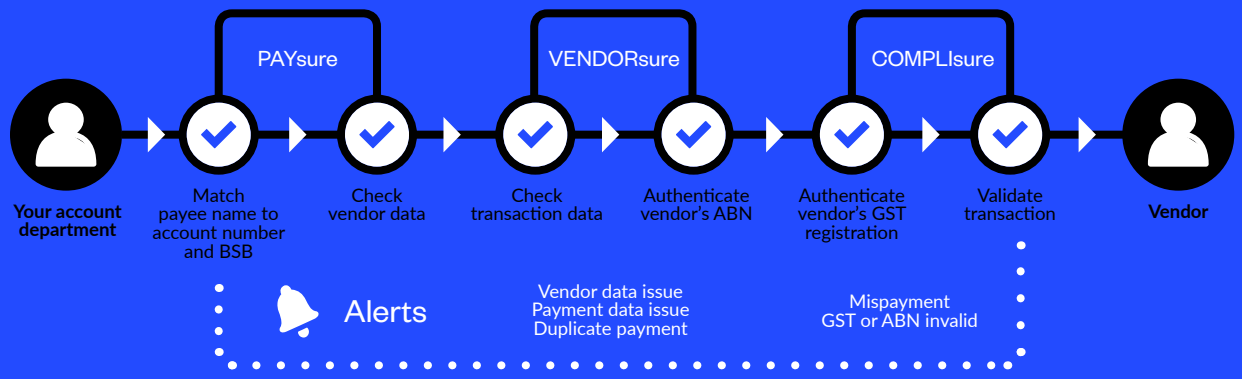
Your suppliers are onboarded through our portal for independent verification. Once that's done, we verify your payment data against an independently maintaines single source of truth built from multiple reference points. When we find anomalies, we alert you so you can investigate and correct them - before erroneous or fraudulent payments are made.

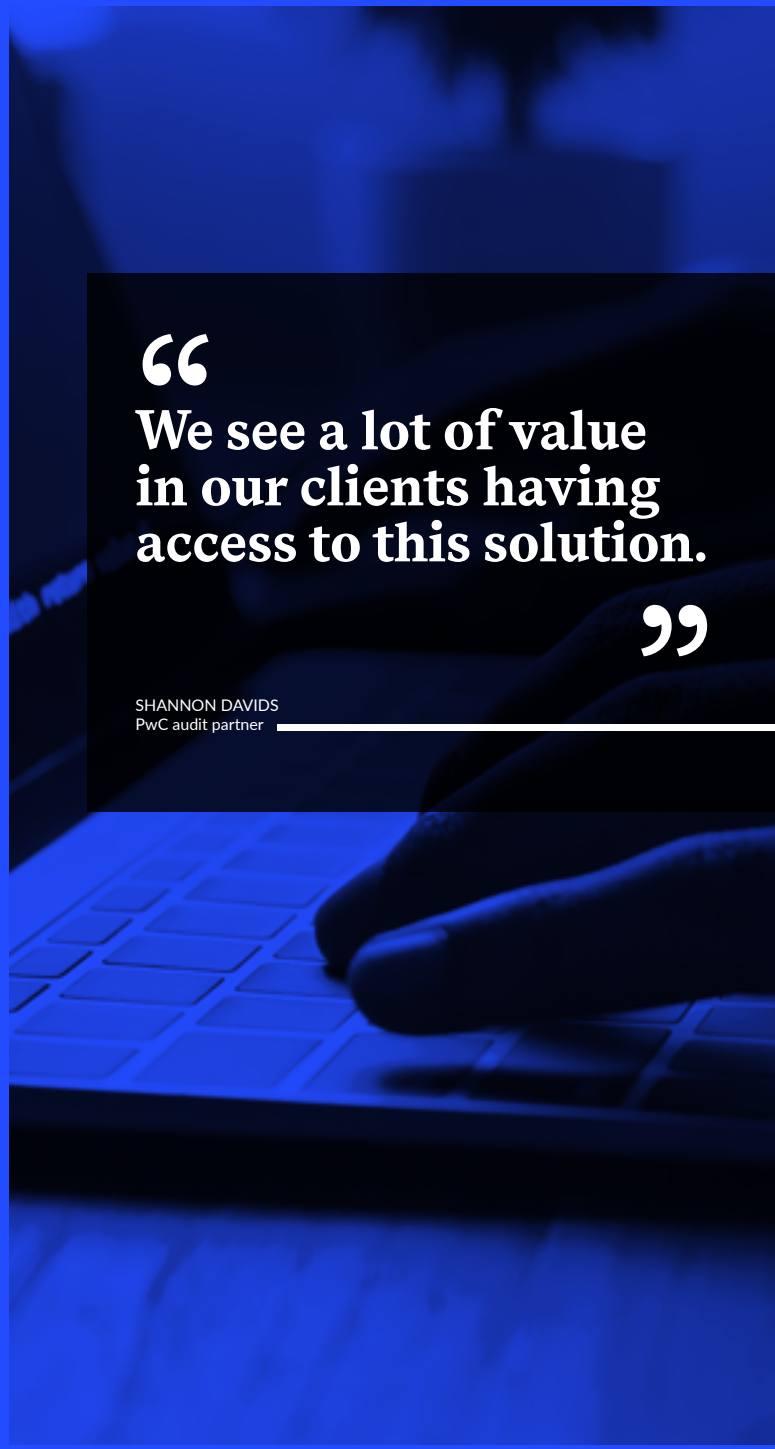
Backed by the best

In 2017, we raised $2m in venture capital to develop our products further. We also partnered with PwC, one of accounting's biggest names, to take our innovation to more customers.

eftsure behind the scenes

We validate the integrity of your online transactions and vendor data in real time and flag any problems so your accounts team can follow up. We also monitor for duplicate payments and other common errors and flag them before payments are made.





> "We see a lot of value in our clients having access to this solution."
>
> SHANNON DAVIDS
> PwC audit partner

Benchmark your VMF today

The first step to payments integrity is a clean VMF. How clean is yours?

Discover how your VMF compares to industry benchmark standards. Visit eftsure-vmfscorecard.com to request your company's scorecard and learn where your organisation is at risk.

Contact us
1300 985 976
sales@eftsure.com.au
eftsure.com.au

Sydney
Level 6
122 Walker Street
North Sydney NSW 2060

Melbourne
Level 40
140 William Street
Melbourne VIC 3000

Brisbane
Level 36, Riparian Plaza
71 Eagle Street
Brisbane QLD 4000

Your first line of defence against fraud and error

eftsure