

The logo for PaymentWorks, featuring the word "Payment" in white and "Works" in a light blue color, with a stylized blue and green circular graphic element between the two words.

PaymentWorks

Payments Fraud and Your Vendor Master: Uncovering Hidden Risks

Digital Supplier Onboarding for Secure,
Compliant and Optimized Business Payments

Presenter



Dan Jurgens
PaymentWorks

Regional Sales Director
dan.jurgens@paymentworks.com

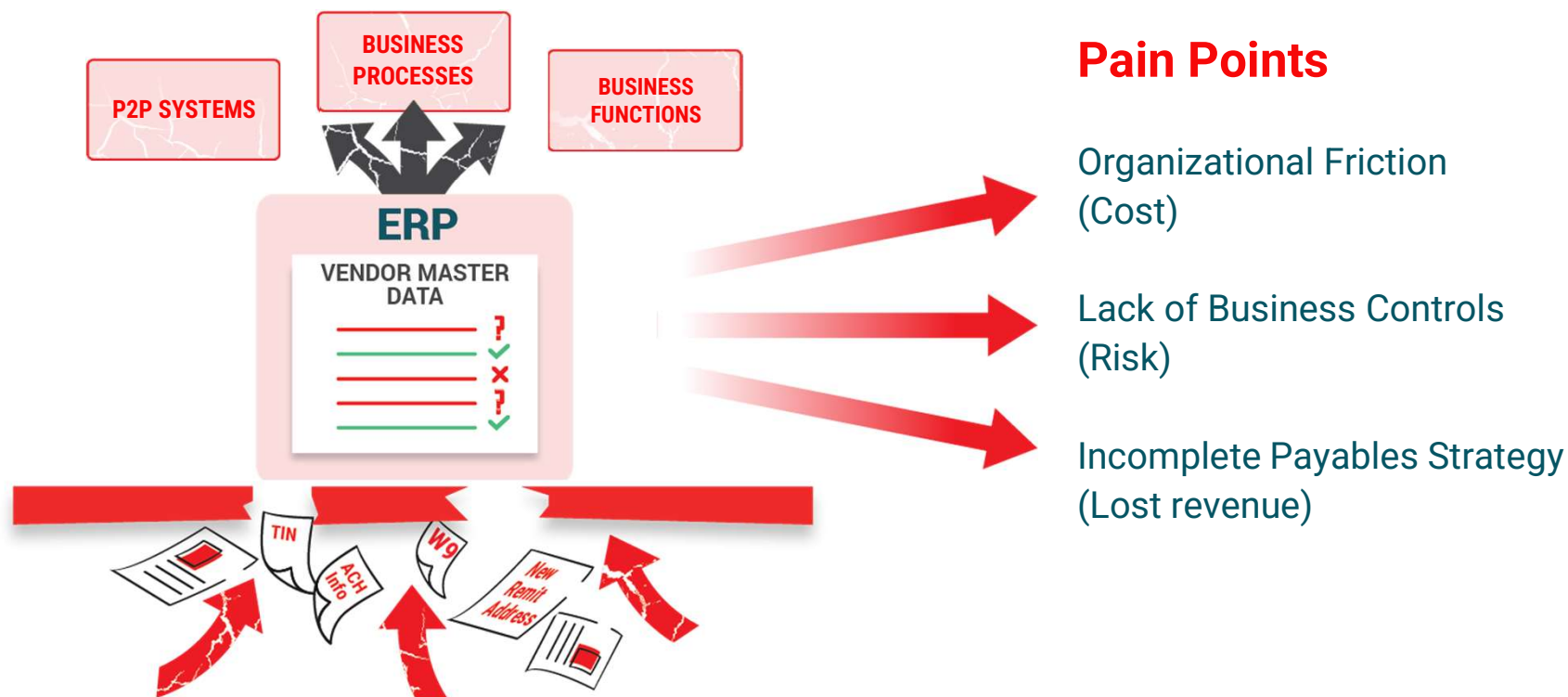
Agenda

- The Fraud Landscape
- The Scams
- What you can do TODAY

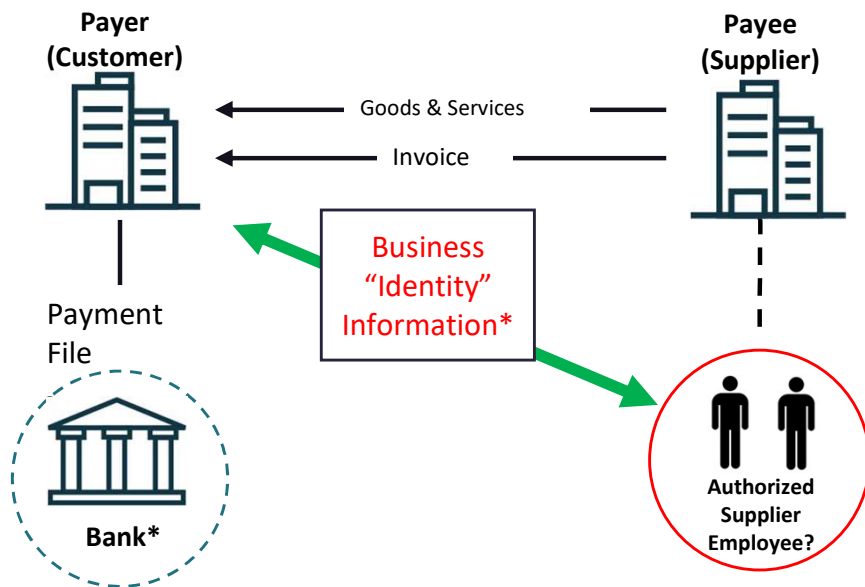


PaymentWorks digital supplier onboarding is the **foundation** of vendor master data management - enabling organizations to **control costs and risks** while executing a payables strategy to **optimize the time value of money**.

The Current Vendor Master File Management Paradigm



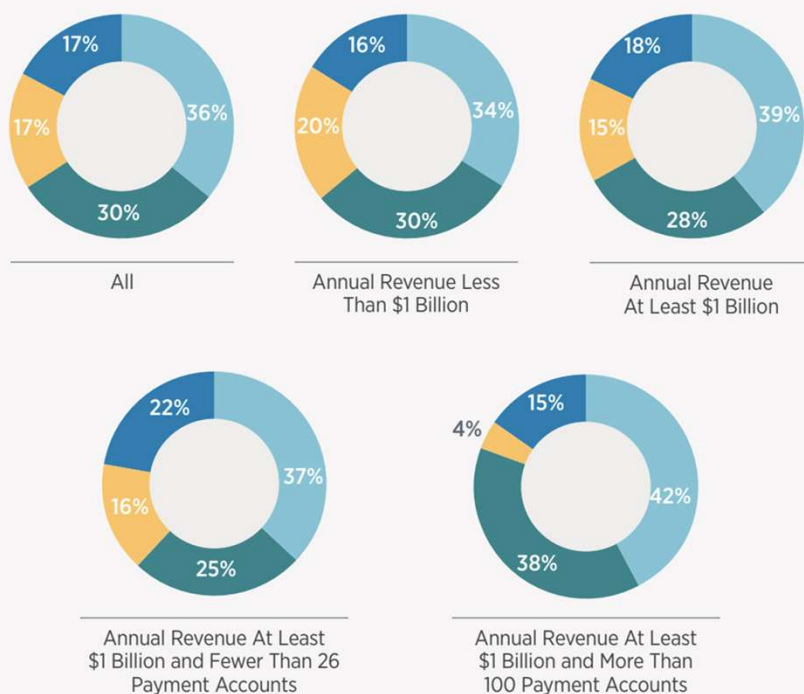
What We Are Seeing



- Identity Information is difficult to verify!
- 99% of organizations collect identity information manually.
- Distributed procurement environments make Business Payments Fraud even more challenging.
- Ownership and governance of Business Payments Fraud isn't implemented until there's a loss.
- Financial losses are not the only risk.
 - Reputational risk
 - Regulatory risk

Validating Beneficiary Payment Information

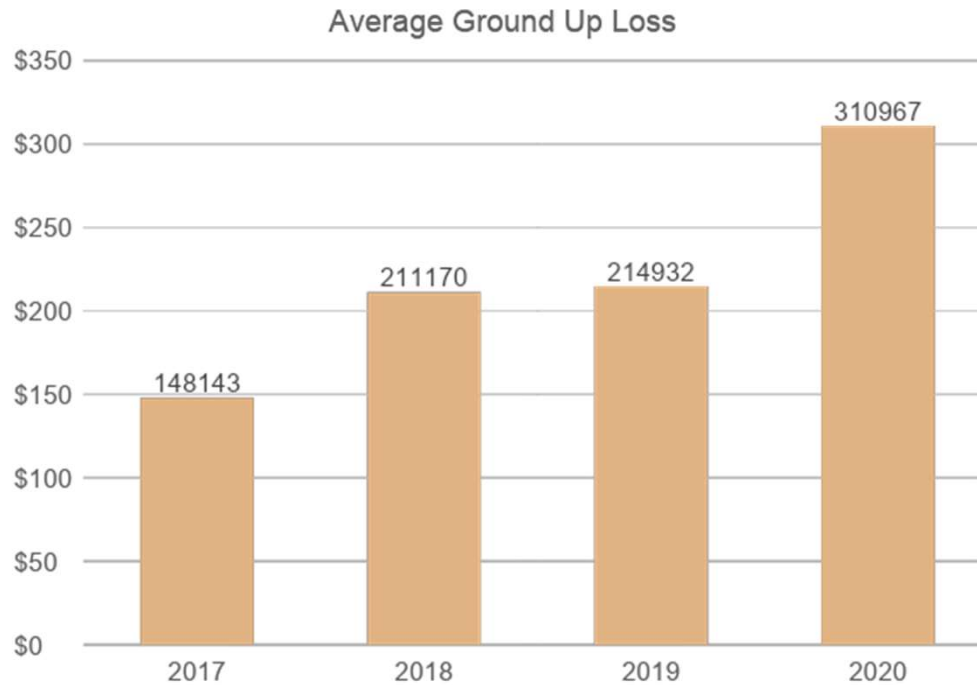
Percentage of Organizations that Validate Beneficiary Payment Information
(Percentage Distribution of Organizations)



- Rely on our financial vendor/bank to validate beneficiary payment information
- Organization uses an external service to validate beneficiary payment information
- Do not validate beneficiary payment information
- Other

Association of Financial Professionals, 2022 Payments Fraud and Control Survey

... and what to consider



Chubb Insurance proprietary Claims Data

- Fraud victims have suffered nearly \$140M in losses since 2017, the **vast amount being uninsured**.
- Losses stem from failing to make a verification attempt or using email to conduct “verifications”.
- Average ground-up loss to businesses and organizations has doubled!

Losses: The Reality



700+ claims
analysed

Average loss \$950k

Median loss \$170k

Largest loss \$40m

Total sum of losses \$290m



Willis Towers Watson Proprietary Claims Data

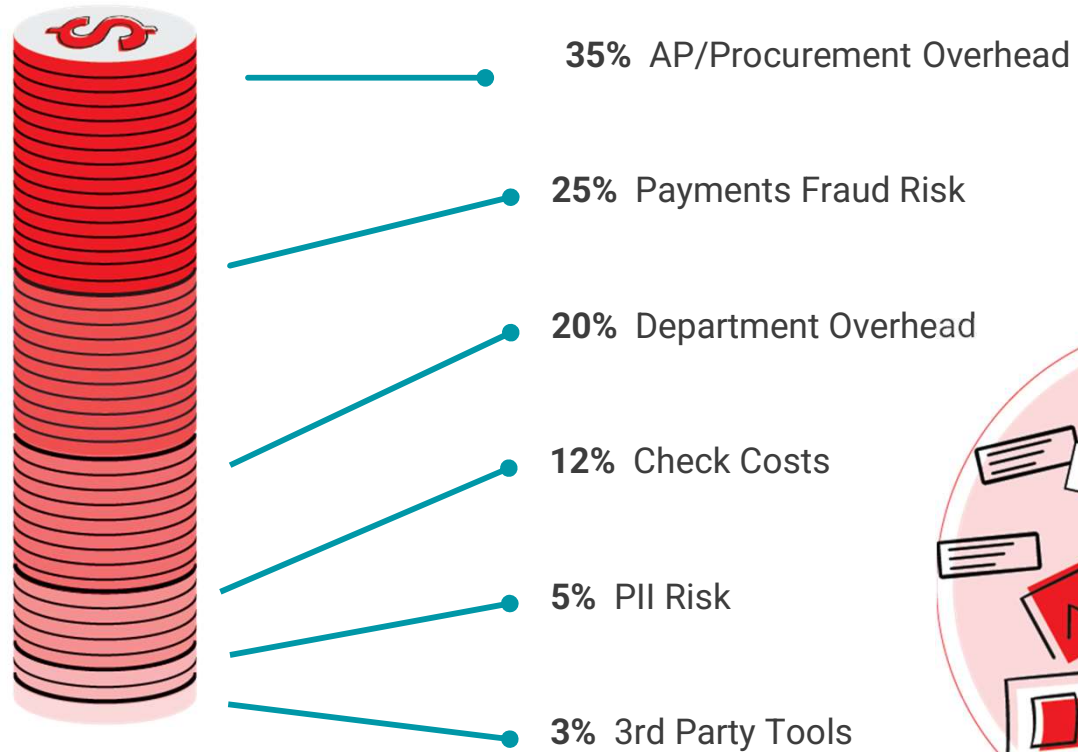
Types of social engineering losses



The Costs and Risks

Cost to Onboard/Maintain a Supplier Per Year

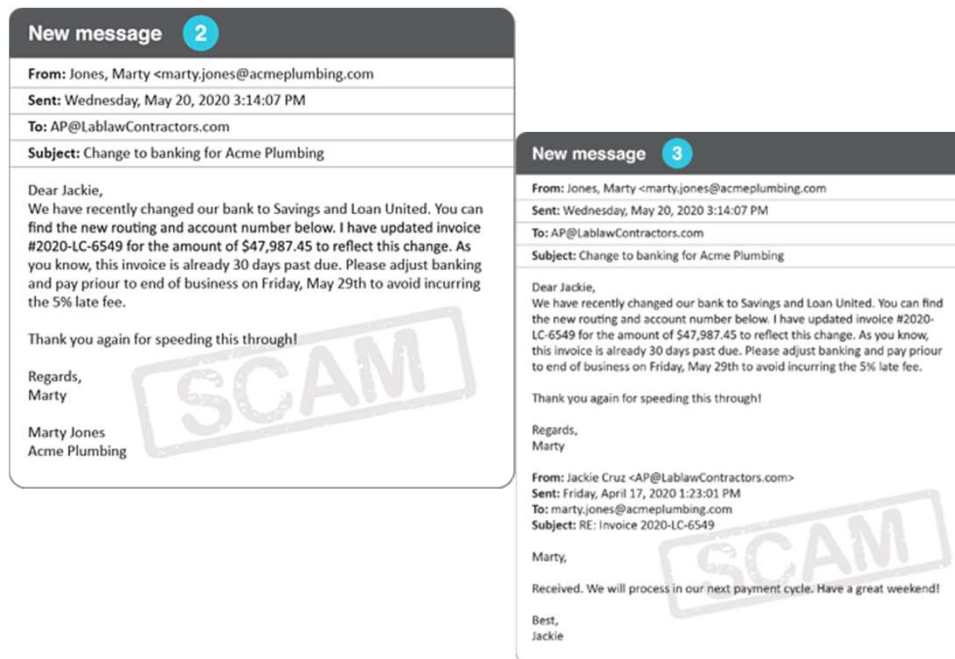
Average: \$100 - \$200 per Supplier*



*PaymentWorks Network and Customer Data 2021-2022

The Scams

Example – Vendor Email Compromise



Steps:

1. It begins by infiltrating your vendor's email (1), usually by way of malware- getting an employee at Acme Plumbing to inadvertently click on a link that grants the fraudster the ability to access and control the email accounts of certain (or all!) employees at Acme.
2. When they have gathered enough information and have the time to know when a big invoice is due to be paid, they strike, almost always adding an additional touch of urgency.
3. Everything about this email seems perfectly legit. The name and address match with what you have been corresponding with all along. The attached invoice is identical. There is very little, if anything, to indicate this email is not from Marty Jones at Acme Plumbing.
4. Taking it further, a fraudster may also opt to add authenticity by following up on previous correspondence.
5. The fraudster's invoice and late fee knowledge, coupled with the email being a response to a previous thread are usually enough to push through a \$47,000 payment to the wrong bank account.

PaymentWorks ANATOMY OF A FRAUD

CUSTOMER:

A midwestern college with multiple campuses

THE FRAUD TYPE:

Domain Spoofing

HOW PAYMENTWORKS CAUGHT IT:

email address did not match company domain

AMOUNT SAVED:

\$935K payment

THE STORY

During a major construction project, the main contact at the college received an email from what appeared to be the vendor requesting to update their ACH information on file. The construction vendor had been working with the college for years, but had not yet onboarded with PaymentWorks.



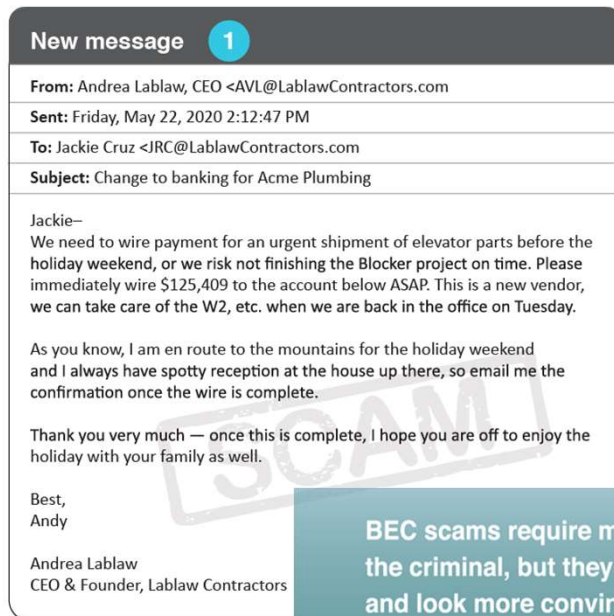
The employee who received the email followed their internal process and responded to the email that they will need to register with PaymentWorks in order to make any changes to their bank information. The initiator then sent an invitation to the email address they had been communicated with.

The fraudster then registered with PaymentWorks.

During regular review, our process caught that there was an extra letter in the email domain that did not match the company website domain. After further review of the registration our analyst uncovered that the domain with the extra letter had been registered just days before, created for the intent of defrauding customers of this construction company.

We rejected the submission, alerted the actual vendor to the activity, and stopped the fraud attempt.

Example – The Evolving Business Email Compromise



BEC scams require more time and effort for the criminal, but they're often more personal and look more convincing to the victim—and as a result, they can yield more profit for the scammer.

— FBI Internet Crime Complaint Center

Steps:

1. One of the most effective means of stealing funds is to have the direction come from within one's own company.
2. In these cases, much like vendor email compromise, a fraudster gains access to a company's email system by getting an unwitting employee to click on a link. Once they have access, they watch and wait. When they see a big vendor payment coming due, they strike, as always, adding specific and significant real details to sell the fraud.
3. Everyone at the firm likely got an email from the CEO letting them know she would be out for the holiday weekend, and that she could only be reached by email. Everyone also likely knows about her house in the mountains. What we have now is an AP staff who might know that to do this is breaking protocol on the vendor setup and account verification process, but the CEO is asking, and making it not only real but also urgent to comply.

What You Can Do Today