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

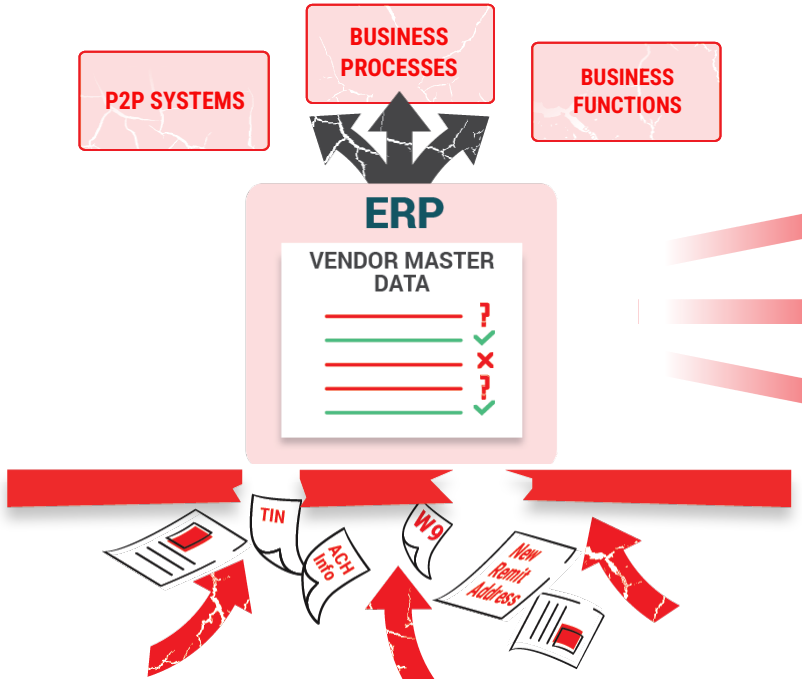
Agenda

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

PaymentWorks

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



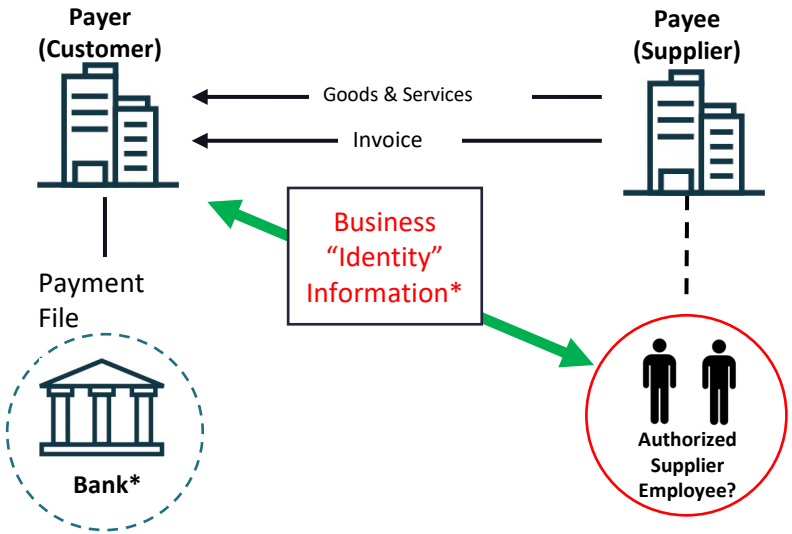
Pain Points

Organizational Friction
(Cost)

Lack of Business Controls
(Risk)

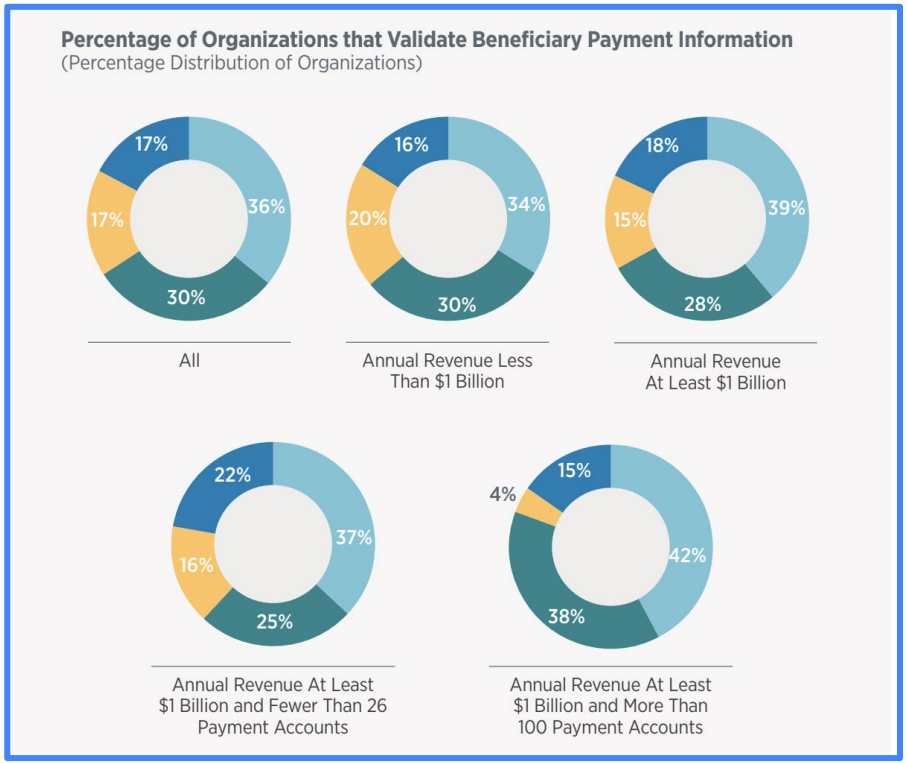
Incomplete Payables Strategy
(Lost revenue)

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

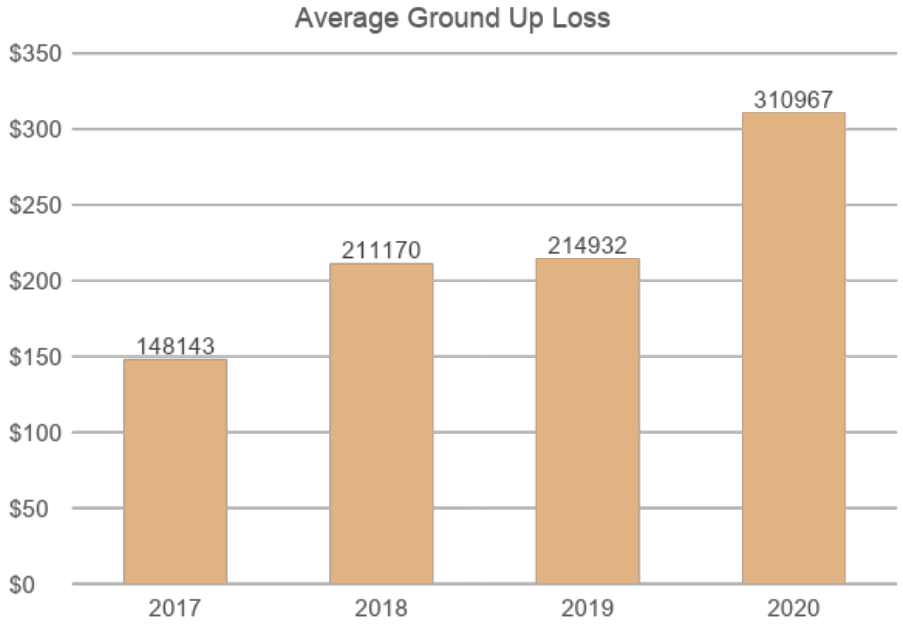
Validating Beneficiary Payment Information



- 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

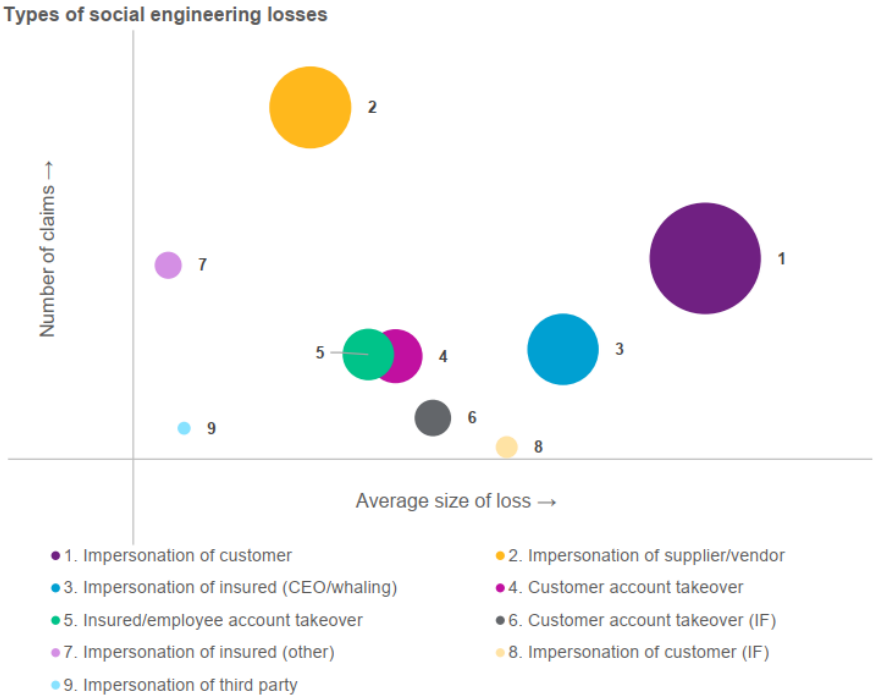
700+ claims analysed

Average loss $950k

Median loss $170k

Largest loss $40m

Total sum of losses $290m



Willis Towers Watson Proprietary Claims Data

The Costs and Risks

Cost to Onboard/Maintain a Supplier Per Year

Average: $100 - $200 per Supplier*

35% AP/Procurement Overhead

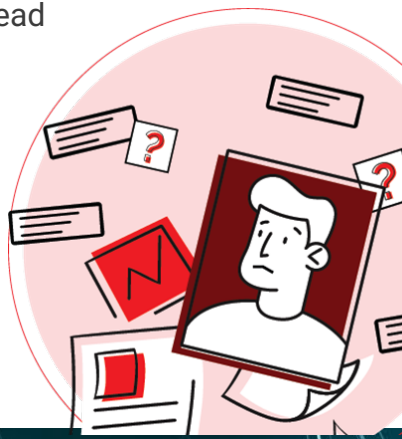
25% Payments Fraud Risk

20% Department Overhead

12% Check Costs

5% PII Risk

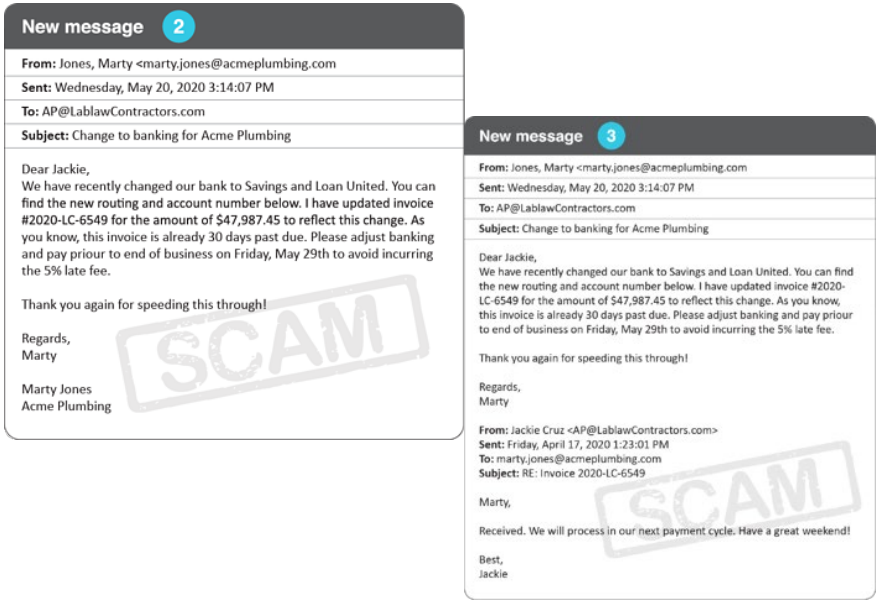
3% 3rd Party Tools



**PaymentWorks Network and Customer Data 2021-2022*

The Scams

Example – Vendor Email Compromise



New message 2

From: Jones, Marty <marty.jones@acmeplumbing.com
Sent: Wednesday, May 20, 2020 3:14:07 PM
To: AP@LablawContractors.com
Subject: Change to banking for Acme Plumbing

Dear Jackie,
We have recently changed our bank to Savings and Loan United. You can find the new routing and account number below. I have updated invoice #2020-LC-6549 for the amount of $47,987.45 to reflect this change. As you know, this invoice is already 30 days past due. Please adjust banking and pay priour to end of business on Friday, May 29th to avoid incurring the 5% late fee.

Thank you again for speeding this through!

Regards,
Marty

Marty Jones
Acme Plumbing

SCAM

New message 3

From: Jones, Marty <marty.jones@acmeplumbing.com
Sent: Wednesday, May 20, 2020 3:14:07 PM
To: AP@LablawContractors.com
Subject: Change to banking for Acme Plumbing

Dear Jackie,
We have recently changed our bank to Savings and Loan United. You can find the new routing and account number below. I have updated invoice #2020-LC-6549 for the amount of $47,987.45 to reflect this change. As you know, this invoice is already 30 days past due. Please adjust banking and pay priour to end of business on Friday, May 29th to avoid incurring the 5% late fee.

Thank you again for speeding this through!

Regards,
Marty

From: Jackie Cruz <AP@LablawContractors.com>
Sent: Friday, April 17, 2020 1:23:01 PM
To: marty.jones@acmeplumbing.com
Subject: RE: Invoice 2020-LC-6549

Marty,

Received. We will process in our next payment cycle. Have a great weekend!

Best,
Jackie

SCAM

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.

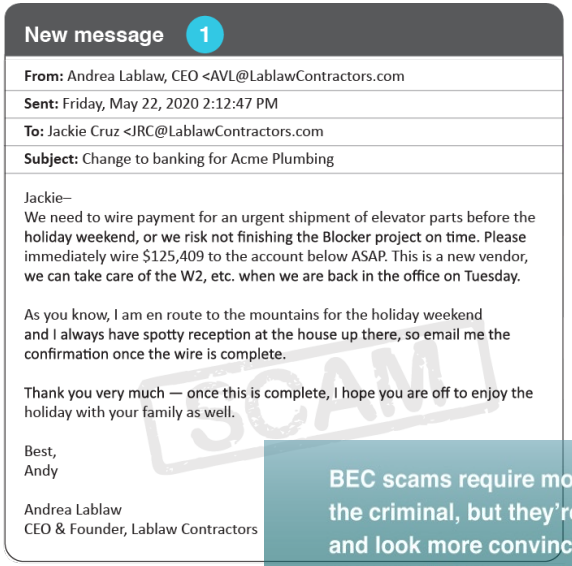
The employee who received the email followed their internal process and responded to the email that they will need to register with PaymentWorks in order to make any changes to their bank information. The initiator then sent an invitation to the email address they had been communicated with.

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



New message 1

From: Andrea Lablaw, CEO <AVL@LablawContractors.com

Sent: Friday, May 22, 2020 2:12:47 PM

To: Jackie Cruz <JRC@LablawContractors.com

Subject: Change to banking for Acme Plumbing

Jackie–
We need to wire payment for an urgent shipment of elevator parts before the holiday weekend, or we risk not finishing the Blocker project on time. Please immediately wire $125,409 to the account below ASAP. This is a new vendor, we can take care of the W2, etc. when we are back in the office on Tuesday.

As you know, I am en route to the mountains for the holiday weekend and I always have spotty reception at the house up there, so email me the confirmation once the wire is complete.

Thank you very much — once this is complete, I hope you are off to enjoy the holiday with your family as well.

Best,
Andy

Andrea Lablaw
CEO & Founder, Lablaw Contractors

SCAM

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

Stop Relying on Bank Letterhead and Voided Checks

Why?

- Letterhead and voided checks can be easily forged.
- They offer not proof of account ownership.
- When transmitted via email, they can be easily intercepted and swapped out.

Rethink Those Vendor Calls

Why?

- Verifying outgoing phone number ownership is (somewhat) easy. Verifying incoming phone number is not.
- Post Covid = lots of VM; VM can be forwarded to email. Email can be hacked.
- Incoming ‘call back’ = no certainty of who you are speaking with.
- Burner phones are a real thing!

Re-examine Your Existing Controls

Why?

- Fraud techniques and compliance requirements change all the time- is the process up-to-date?
- Is it being followed?
- Is it insurable? Can it be audited?
- Does it rely on a human being 100% right all the time?
- Is your 3rd party provider covering ALL bank account changes? Is it verifying ownership?

What to Ask

- Does our current crime insurance policy cover losses if I am tricked by a fraudster and send money to the wrong account?
- Are there scenarios where a mistake I make is not covered?

What to Know

- Most policies require coverage for this type of loss to be affirmatively added.
- When included, limits are generally very low.
- Coverage is difficult to obtain due to rising losses.

The PaymentWorks Platform

Digital onboarding for secure, compliant and optimized business payments.

Requested by payer

Payer/Customer

- Payment Method
- Payment Terms
- Tax Classification
- Addresses
- Diversity
- Insurance COIs
- Conflict of Interest
- Sanction Monitoring
- Compliance Certs

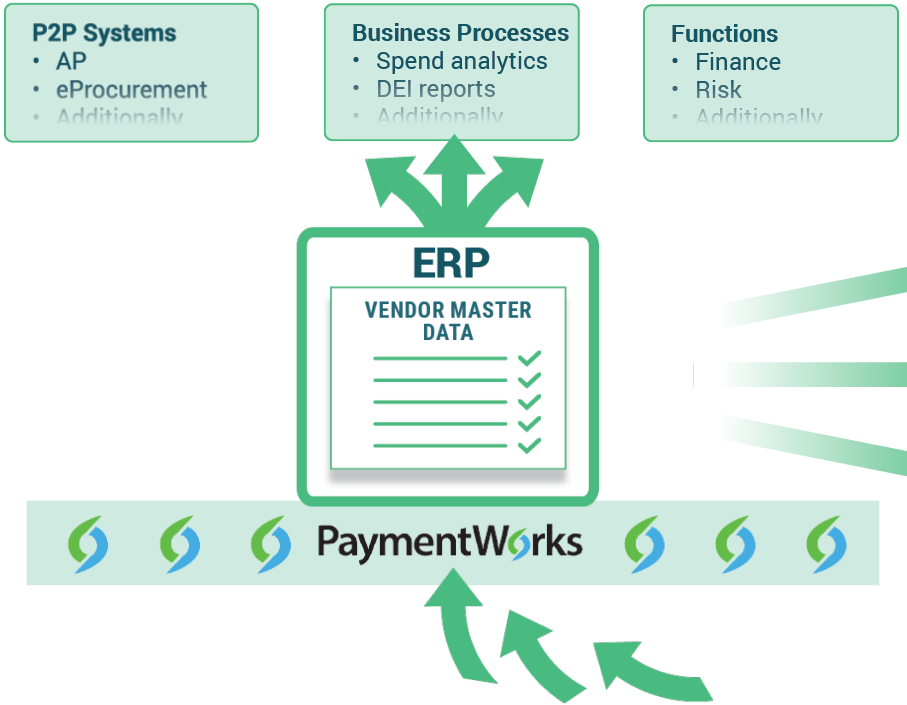
Maintained by payee

Payee/Vendor

Workflows | **3rd Party Data Checks** | **Fraud Protection** | **Network Intelligence** | **ERP Connectors**

PaymentWorks

The PaymentWorks Paradigm: A Solid Foundation



Results

Automate Onboarding and 3rd Party Checks

Eliminate Risk of Losses to Fraud, Lock Down Compliance

Convert Vendors to Electronic Payment Types

What Sets Us Apart

Controlled Costs	Reduced Risks	Optimized Payments
• Automated 3rd party checks • Onboarding Tracker® for complete visibility • Support and reporting	• Risk transfer for fraudulent ACH payments • Auditable business controls • Collection point for all compliance documentation (e.g., sanctions checks, insurance docs, conflicts of interest, etc.)	• Payment strategy married to onboarding process • Lever to drive adoptions of electronic payments • Reporting and analytics

Questions?