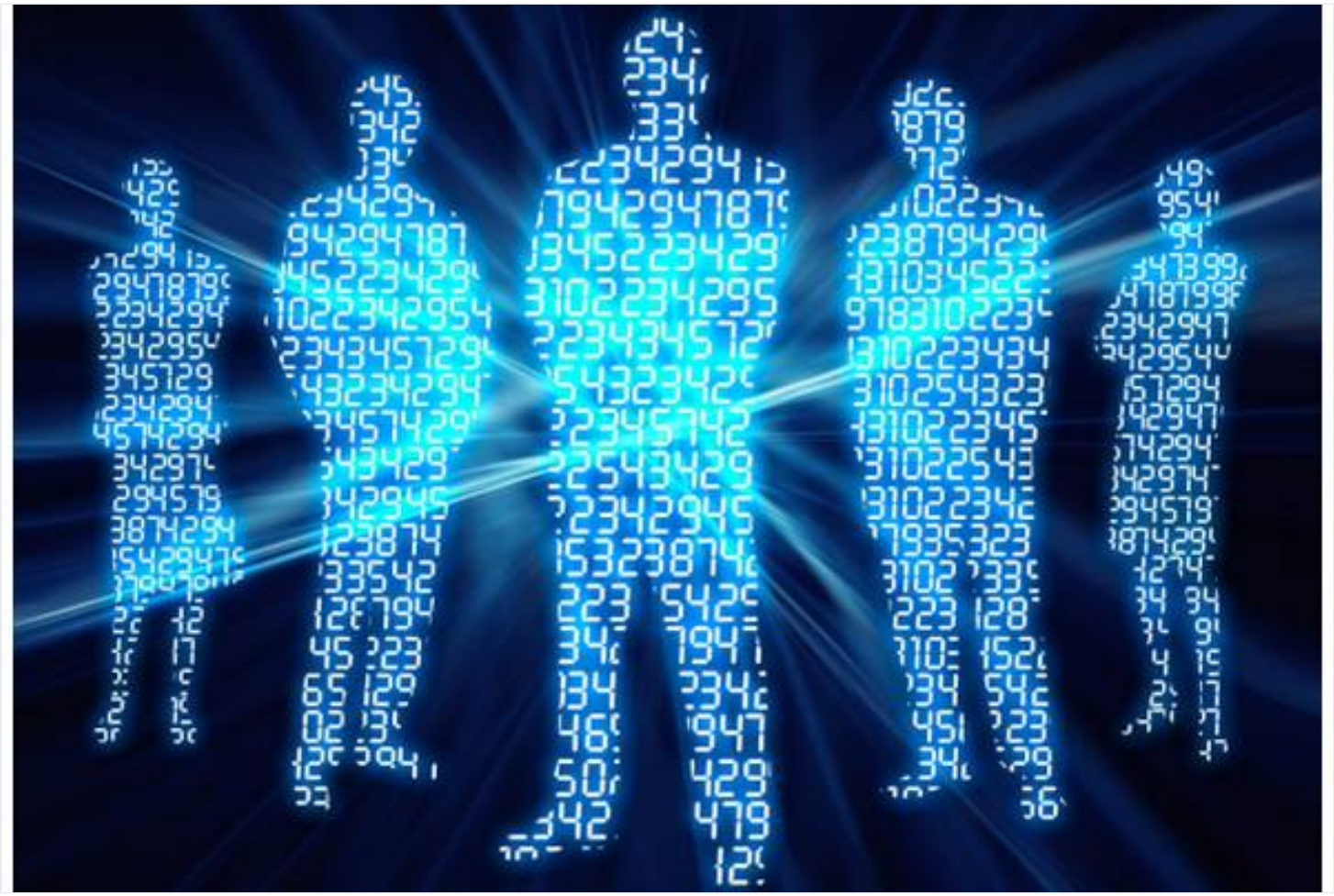
mortar" approach, instead they're built from the ground up with digital and global operations in mind. The phenomenon began with ecommerce and adtech - essentially the ...

Nov. 01, 2017



Modern businesses with high growth targets no longer use the slow-build "brick and mortar" approach, instead they're built from the ground up with digital and global operations in mind. The phenomenon began with ecommerce and adtech – essentially the first time you bought something on a website or saw a banner ad.

Those companies may have paved the way, but digital global operations are now

which these businesses could use help with is managing accounts payable risk. With these hyper-growth companies, suppliers, partners, vendors, and service providers are added quickly and at high volumes. Because these suppliers are seen as critical partners, companies' CEOs, COOs, and CFOs are not going to tolerate time-intensive, manual background checks and procurement sourcing. That volume, reach, and speed requires greater resiliency against risk and fraud which comes from scaling faster. And it's all multiplied if these partners are overseas.

Table 1 shows the top countries where we detected fraud incidents (an attempt to pay that was halted due to a questionable payee where there was an OFAC SDN hit or other algorithmic fraud-based red flag). This data is based on Tipalti's remittance on behalf of our clients to over 190 countries, across nearly 2 million payees, and thousands of payments each month.

Table 1. Top 20 Countries with Most Fraud Activity (and at least 1,000 payment attempts)

Country	Fraud Incidents
Indonesia	12.26%
Vietnam	5.72%
India	0.91%
Cambodia	0.60%
Malaysia	0.58%

Singapore	0.55%

Bangladesh	0.31%
Pakistan	0.31%
Brazil	0.27%
Nigeria	0.26%
Australia	0.22%
Ireland	0.19%
Japan	0.18%
Netherlands	0.16%
France	0.16%
Thailand	0.15%

As the data shows, fraud attempts are more prevalent in certain countries, and those countries may legitimately be considered more risky. Yet, fraud can come from anywhere. "First world" friendly countries like Australia, Ireland, Japan, the Netherlands, and France are clearly home to fraudsters in the supplier chain, based on this data. So while certain regions are more risk-prone, the best policy is one that considers every region regardless of where you "think" there may be risk.

While sub-one-percent fraud rates may seem insignificant, consider that digital companies are making thousands of payments a month. That's a considerable risk

exposure. Beyond just losing out on a fraudulent payment, if these end up to be OFAC

Therefore, businesses need to be able to support more auditable electronic payment methods and encourage payees to use them.

Unfortunately, digital payments are also increasingly at risk as well. And these electronic payment methods are harder to recover from in the face of fraud. The funds may have already moved on from their landing spot, and their accounts closed before the company notices. Across borders or certain payment methods, it might not even be possible.

Wire transfers are generally reserved for high-value transactions because of their cost. But due to their larger amounts and the virtually instantaneous point in which funds land, the impact of fraud should be weighted. Wire fraud has also increased in five years from 5% of companies experiencing it to 46% (AFP 2017 Payments and Fraud Control Survey). This is all the more reason to be careful, as recovery from wire fraud is itself complex and expensive.

Because Tipalti remits through multiple payment methods, we've been able to determine that certain payment methods are more susceptible to fraud (see Table 2).

Table 2. Payment Method Fraud Propensity

Payment Method	**Fraud Incidents**
eWallets	1.00%
eCheck / International ACH	0.20%
Wire Transfers	0.19%
Paper Check	0.09%

US ACH	0.01%

wire transfers, but at a lower cost in exchange for a little bit more remittance time. They may be an acceptable alternative to wires.

Bottom line, businesses need to do what they can **prior to payment** by identifying and validating their payees. There are several key steps a company can take to do this:

- Validating payment data at onboarding
- Collecting and validating tax forms and IDs
- Shifting supplier payment behavior away from checks and wires to safer digital payment methods
- Checking against OFAC and sanctions lists at onboarding and prior to each payment
- Proactively looking for fraud patterns
- Instituting a systematic invoice and payment approval workflow
- Instituting role-based views and access to payables data
- Ensuring audit trails for all payment related activity by not only finance users but also suppliers
- Centralizing visibility into all banking infrastructures across global business units, entities, and subsidiaries

An extra note about using tax identification as a fraud deterrent: Tax identities are required by the IRS to meet FATCA requirements (W-9 for domestic, W-8 series forms for international partners) and for VAT countries – so you should be doing it anyway. But requiring payees to provide this information during onboarding is an added insurance policy to identify who the payee is. Collecting this information before any payments are made rather than at the end of the year also ensures that if the partner changes addresses or stops being a partner, the information is retained.