PAYMENT *Fraud*

Assessing and Responding to an Escalating Threat

Underwritten by

coupa

An eBook written and produced by

Strategic Treasurer

Contents

An All-Out War

Many of the risks that treasury guards against, from market fluctuations to currency devaluation, are impersonal, passive threats that can affect the value of assets incidentally. While these passive threats are dangerous and complicated enough, treasury faces one very intentional threat: fraud. There is nothing incidental about this risk. More than idly threatening liquid assets and data, cyber criminals are waging all-out war against organizations.

In such a war, there is no room for uncertainty regarding roles. Everyone must know their responsibilities. Unfortunately, the responsibilities for payment security can be scattered and unclear, and treasurers often find themselves unsure what role they are to play. They realize that payment fraud is a significant risk, and they know they must manage risk. That said, however, the mechanics of payment security fall at least partially to other departments, such as IT.

This situation raises an important question: *What is the treasurer's role in managing the risk of payment security when some parts of the enactment of payment security fall outside the treasury function?*

To draw an analogy, the proper role of the treasurer in payment security is that of superintendent. The superintendent in a school does not drive the bus, teach all the children or perform custodial services. However, the superintendent is responsible for making sure all these tasks are being performed and are meeting or exceeding standards.

In the same way, treasury is not in charge of everything. Treasury does not choose what firewall to buy, make all the payments, set the router passwords or install the access card system at the entrance points to the building. To appropriately guard organizational liquidity, however, treasury bears a responsibility to keep watch over all elements that affect payment security, even if those elements themselves are not their responsibility.

Since this may be easier said than done, we'll discuss more details surrounding the appropriate performance of treasury's role as superintendent of payment security in a later section. For now, however, it's clear that to carry out this role, treasury must keep abreast of news in the war on fraud and must be involved and proactive in leading their organization's tactics. This eBook is intended as a tool to that end, helping treasury to understand the current situation, the threat levels of various types of fraud, common areas of vulnerability, and frameworks and tactics for constructing a solid defense.

> More than idly threatening liquid assets and data, cyber criminals are waging all-out war against organizations.

Many organizations, it appears, are not quite as secure as they think they are.

The Current Situation

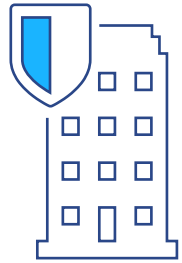
To understand the current situation surrounding fraud and the efficacy of average organizational defenses, begin by noting the following statistics:

ACCORDING TO A SURVEY IN EARLY 2020

of companies had experienced fraud over the course of the past year. This number sat at 52% for both 2018 and 2019.

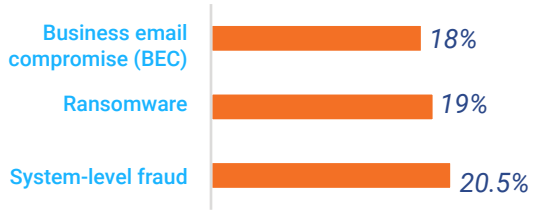
76% *of respondents to a 2020 survey answered that they felt the threat level of fraud had increased or significantly increased in the past year.*

When asked to rate their organizational position with regards to fraud compared to the prior year, ***56%*** *stated that they were in a better or significantly better position.*



The most common type of fraud attempted, with ***9*** *out of* ***10*** *firms reporting attempts in 2020 , was business email compromise (BEC), also known as CEO or imposter fraud. System-level fraud and ransomware, two types of fraud that are much less common than BEC but can incur some of the most sizable losses.*

SUCCESS RATES



Ransomware's losses were never paltry, but they rose by a factor of ten in 2019.

Q4 OF 2018	*The average loss was around $10,000.*
Q4 OF 2019	*The average payoff was $84,116.*
Q1 OF 2020	*Continued the trend with an average of $111,605.*

Given the high attempt rates, rising success rates for some of the most devastating fraud types, and payoffs soaring tenfold in less than two years, it is no wonder respondents perceived the threat levels as increasing. What is surprising, however, is that respondents, for several years of rising fraud rates, have persistently answered that they considered their position with regards to fraud as better than in the prior year. In light of each year's results, this seems overly optimistic. Many organizations, it appears, are not quite as secure as they think they are.

The outlook for cybercriminals, on the other hand, is unfortunately quite rosy for the time being. They have found elements that work in their favor and have learned how to operate efficiently. Some characteristics of the cybercriminal's methods are listed below:

- **Persistent:** Criminals are not giving up and are constantly adjusting and attacking via various methods, patiently trying until they find an angle that works.
- **Automated:** Criminals are showcasing the usefulness of automation for increasing efficiency and effectiveness. They use software to continually probe potential victims and uncover weaknesses, putting every organization at risk at all times.
- **Sophisticated:** As criminals notice the ways we identify and avert their attempts, they grow more sophisticated in covering their tracks, making their social engineering believable, and using more intricate technology. Rather than sending emails from unfamiliar names and trying to invent a convincing scenario, for example, they now lower the recipient's guard by spoofing a trusted email address.
- **Targeted:** Once the criminals have identified weaknesses in an organization, they begin other activities custom-tailored to maximize yield. It's important to realize that while your organization is constantly being prodded by broad, non-specific attacks, it is also being analyzed individually, its weaknesses assessed, and plans made to exploit any vulnerability found.
- **Adaptive:** Existing attack methods don't stop, but new methods are added, and adjustments are made to keep these methods effective in the ever-changing environment.

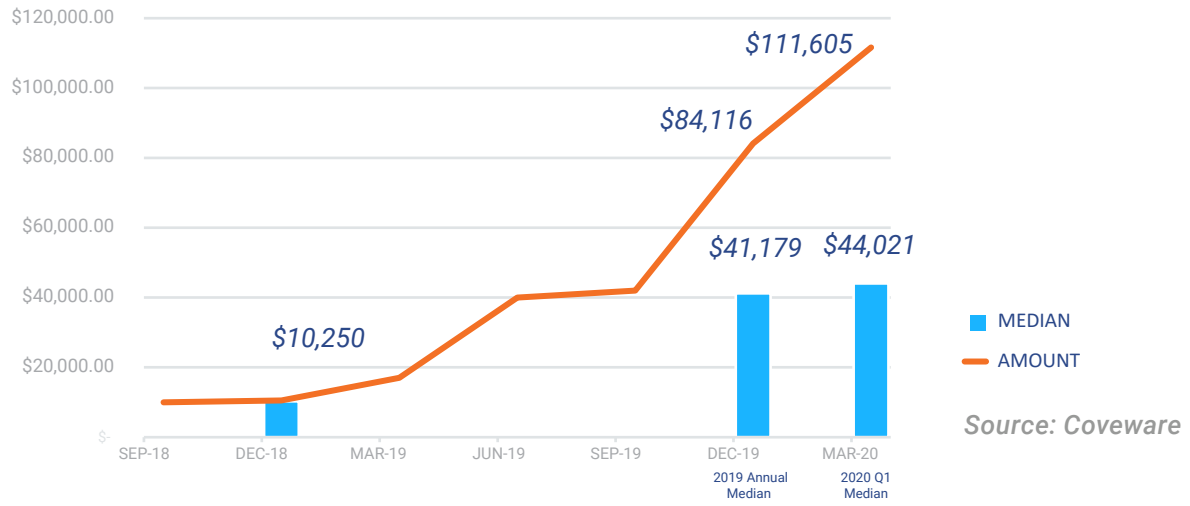
Results Are the Feedback Loop

Crime is paying—and the payoff amounts are growing larger and larger as time goes by. Ransomware's 1-year jump from $10,000 to over $100,000 creates the most striking example of this, but it isn't the only method yielding more as the years pass.

This creates a positive feedback loop for criminals. They develop and adapt using more sophisticated methods. As a result, their success rates increase, and they can steal more funds and data more often. With ample funding as a result of their successes, criminals have the resources they need to improve their infrastructure, tools, automation and methods once again.

They also have the luxury of patience. They can increase their sophistication even more, and they can wait out a company, watching for the right moment. At other times, they put in the work to steal encrypted data with the confidence that someday, technological advances will allow them to crack the encryption, and their work now will pay off then. These efforts and improvements all breed greater success, and the cycle continues.

AVERAGE PAYMENT MADE BY RANSOMWARE VICTIMS



Source: Coveware

Adapting Methods and Leveraging Technology: What Can Cause You to Never Sleep?

If the problem with fraud were simply that criminals had a single, highly effective method, our response could be simple, focused and ultimately successful. We would have far less to worry about. This, however, is not the issue.

The problem we face is that fraud escalates. Criminals learn more and leverage more, and what they learn in one environment they apply to others as well. Our responses are then scattered, uncertain and frequently a step or two behind the highly proactive criminals. This does not mean, however, that there is nothing we can do and nothing we can understand about the patterns of fraudulent action.

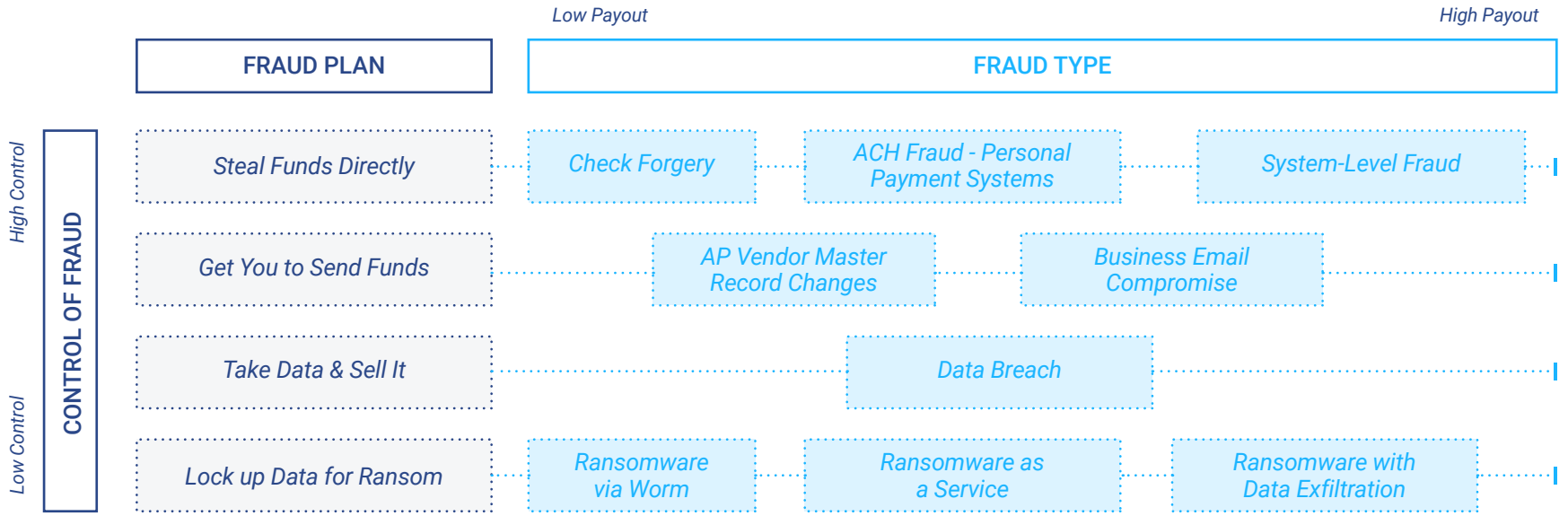
Below are some elements of fraud that change more slowly than the exact methods used.

The Criminal Playbook

1. *First, they try to steal funds directly from your organization.*
2. *If they can't steal it directly, they will try to convince you to send it.*
3. *If they can't convince you to send funds, they'll try to steal data.*
4. *If they can't steal data, they lock it up for ransom.*

It's a simple flowchart, but at times criminals will combine the above methods to increase their payoff or their chances of success. For example, the two types of attacks on internal data, ransomware and data exfiltration, are often combined. In this scenario, criminals both steal and lock up your data, demanding a ransom before unlocking it again. This creates the possibility of being paid twice for the same data—once by you and once by the black market—and it gives a backup funding avenue in case you refuse to pay them. Since the average payoff has risen so sharply for ransomware, criminals are highly motivated to continue increasing their use of this fraud type.

THE CRIMINAL PLAYBOOK: FRAUD TYPES AND ASSOCIATED INTENTIONS



> Use of artificial intelligence (AI) has allowed criminals to increase the credibility of their scams, compromising the human element even more severely.

As for convincing the organization to send them funds, criminals use social engineering to make staff believe they are sending a legitimate payment. This social engineering can occur by various means. BEC, currently the most commonly attempted type of fraud, is an example of this. BEC frauds involve spoofing the email address of a company's employee, typically a CEO, CFO or other C-Suite executive, and using this identity to convince an employee with payment privileges that a payment must be made urgently.

These emails typically demand the payment be sent immediately without anyone else being consulted and without the payment details in the email being confirmed out-of-band. The manipulation often extends to a threat that the employee could lose their job if they fail to comply. BEC incites fear and confusion, essentially pressuring the employee into a poor decision out of self-protection.

Use of artificial intelligence (AI) has allowed criminals to increase the credibility of these and similar scams, compromising the human element even more severely. "Vishing," a type of fraud where criminals use AI to study and mimic a CEO or CFO's voice over the phone, can be shockingly convincing. In addition, if the recipient of a fraudulent email responds to it, AI can keep the conversation going in a way that makes it seem more legitimate, gaining buy-in from the employee.

All these types of attacks come in addition to direct cyber-attacks on processes, payment systems and files. While more novel fraud types are growing rapidly and gaining attention, classic "hacking," malware, old fashioned check fraud, etc. are in no danger of being replaced by these new types.

Adapting Methods and Leveraging Technology: What Will Let You Sleep

With all of us in treasury up against this highly effective criminal playbook, the task of acting as superintendents for our businesses may seem daunting. This makes it all the more important for us to consider the bigger picture of threat vs. response and to be clear about treasury's role. What options are there that will let us sleep at night?

Just like cybercrime, cybersecurity has many layers. Not all of them are up to the treasurer, but awareness and a sense of ownership should characterize treasury's attitude towards cybersecurity. Just as criminals don't follow just one method or line of attack, treasurers' responses also need to cover many bases. One such base is technology: the ways in which treasury management systems (TMS) and other technology come with built-in safeguards that treasurers can use to underpin their security efforts.

The Treasurer's Playbook: Leveraging Technology

We tend to underestimate just how much support is available to us through technology. Treasurers don't need to be IT specialists and fully understand all the technical details behind a system to know if and how it will help them in their security quest. Instead, there are a few straightforward considerations treasurers should bear in mind when assessing possible payment security solutions.

1. *Consider where and how your payments data is saved.*
2. *Consider the methods for processing your payments data.*
3. *Consider the shape your data takes when processed.*
4. *Consider who has access to your payments data.*
5. *Consider who has permission to approve and release payments.*
6. *Consider how you can control who receives a payment.*

Technological vulnerabilities and associated safeguards

This playbook is a helpful guideline towards the kinds of safeguards a system can offer. In turn, it maps out the technological vulnerabilities that treasurers face when processing payments and that they need to respond to. Finding a viable setup is all about connecting the two: what are the vulnerabilities, and how can you counteract them?

Treasurers want to feel confident about the security of their payments even though—or precisely because some things are out of their hands. They want to know that they can still protect their company, even in the face of such sophisticated threats.

Responding to Vulnerabilities

Technology represents a layer of protection that acts as a sort of built-in background safety net that treasurers don't need to actively worry about. This is not to say that they don't have to develop viable processes that integrate this safety net into their day-to-day tasks and enable it to fully unfold its potential. Technology is never fully independent of what we do or don't do in any particular moment, but it does give us a foundation we can build on. It can alleviate some of the pressure that comes from having to monitor so many potential threats and points of attack.

Treasurers need actionable steps to find the right technological support to free up capacities that can in turn be dedicated to other aspects of cybersecurity. By taking heed of the above considerations and vulnerabilities, treasurers can do just that. If they ask the right questions up front and select technology that complements and enhances their payments setup, they're one step closer to being successful superintendents.

Technological Vulnerabilities	Technological Solutions
Hosting	Cloud solution
Processing	SFTP, API connection
Data exfiltration	Encryption
Access	2FA, SSO, user permissions
Approval	Multiple approval levels
Release	Allow lists/block lists

Regulations, Requirements and Growing Expectations

Criminals have not been idle, but neither has the corporate financial space. In recognition that the ever-growing threats of fraud necessitate more care for the defense, several networks and groups have put regulations in place to protect their members or participants. Similarly, to guard themselves, their partners, and their clients or customers, firms should carefully assess the security status of their own vendors and potential partners and should put requirements in place as appropriate.

Payment Platforms

Each additional payment platform creates additional points of exposure. Conversely, each new member on a payment platform adds some additional exposure for the network. No matter how robust an individual payment platform's own security infrastructure may be, it can only be as secure as the most exposed surface area and the weakest link in its network of members. Every company that collects credit card information and every organization on SWIFT bring their own vulnerability to the platforms. When breaches occur and data or funds are stolen as a result of an unprotected link in the chain, other participants suffer as well, and the payment platforms themselves are often held responsible.

After experiencing these problems, payment platforms are highly motivated to harden the endpoints. This is done by regulating that in order to participate in the platform, organizations must meet certain security requirements. Two of the most prominent regulations are PCI-DSS for payment card security and SWIFT CSP for banks and organizations participating in the SWIFT network.

PCI Security Standards Council

PCI-DSS:

The Payment Card Industry Data Security Standard, shortened to PCI-DSS, was put in place in response to precipitous amounts of card fraud starting back in 2004. Five of the largest payment card groups joined forces and formed the PCI-SSC (Payment Card Industry Security Standards Council), which then issued PCI-DSS. The standard applies to all organizations that accept, transmit or store any cardholder data. Its twelve requirements set a standard for participants' technical security measures, controls and employee training.

SWIFT **Customer Security Programme**

SWIFT CSP:

After a number of banks on the SWIFT network proved to be vulnerable, SWIFT set about hardening their endpoints by creating the Customer Security Programme, or CSP. All organizations on the SWIFT network must comply with this set of mandatory controls and are strongly encouraged to adopt the advisory controls. As of 2020, there are twenty mandatory and ten advisory controls. These include a training component and various measures to protect the surface area of attack.

Originally, SWIFT allowed self-assessment and attestation, but an assessment by an outside party, such as a certified TMS vendor, is now required.

Procurement: Vendor Assessment

All organizations should be mindful and cautious of the risks of doing business with other parties who provide ongoing services or support. While your organization does not necessarily need to issue a set of twelve or twenty requirements for your partners, it is appropriate to mandate certain elements of security in order to protect yourself, your other vendors and your customers or clients.

Security Surveys:

Before partnering with a vendor, it's important to perform due diligence and understand their current level of security. An entry survey should be completed by anyone who will be providing ongoing services or support. The results of this survey should confirm that those entering your network have end-to-end security.

Mandated Vulnerability Assessments and Penetration Testing:

It is advisable to require that your partners have annual vulnerability assessments and penetration testing and that they share the results of these tests with you. A third party should always be involved in such tests and assessments.

SOC1, SOC2 Reporting:

SOC1 and SOC2 reports are designed specifically to confirm that a service organization's internal controls are robust enough to protect their clients. As such, it's highly recommended that you require these certifications from your partners. SOC1 reports verify that your vendor's internal financial controls are adequate and functioning properly. SOC2 reports confirm that the company's cloud and data security controls are up to standard.

ISO 27001:2013:

ISO 27001:2013 is another standard for handling the risk associated with information security. Regulations such as GDPR in the EU have brought up additional risks to managing employee and client information, making it both important and sometimes difficult to ensure information security is adequate. ISO 27001, which has multiple stages, can prove helpful in verifying that third parties manage their data securely.

Security Frameworks and Principles

> With an undertaking as massive, detailed and personalized as finding and defending our own organization's vulnerabilities, it's helpful to have a framework that lays out the principles and basic controls of security.

With an undertaking as massive, detailed and personalized as finding and defending our own organization's vulnerabilities, it's helpful to have a framework that lays out the principles and basic controls of security. Multiple organizations have published such frameworks and principles. Two examples are covered below, but your firm may use others.

NIST Cybersecurity Framework:

One of the most used and accepted frameworks is the Cybersecurity Framework developed by the National Institute of Standards and Technology, or NIST. This framework is now estimated to be in use by approximately half of U.S. organizations.

At the core of NIST's framework are five functions that act as the pillars upon which the rest of the framework is supported:

#1-Identify: This function involves understanding your organization, its industry and context, and its risks and exposures. This requires thorough visibility into various areas within your company.

#2-Protect: The second function deals with implementing the necessary security to "limit or contain the impact of a potential cybersecurity event." This includes elements such as employee training, access control and security software deployment.

#3-Detect: Detection is about taking the proper measures to ensure that when fraudulent activity occurs, it is found quickly. It involves monitoring areas such as payment and user activity via technology solutions and processes.

#4-Respond: This function has to do with taking appropriate action once fraudulent activity has been detected. Important elements of the response include communication, mitigation of the fraud's effects and learning from the event.

#5-Recover: Recovery involves the restoration of a company's systems or services that may have been halted or affected by the fraudulent event. This function returns the organization to normalcy while implementing any necessary changes.

Strategic Treasurer's 12 Security Principles:

We also recommend the 12 Principles for Payment Security, a framework that covers both the basic and less commonly identified practices characteristic of a strong defense for payments.

1. *Speed Matters*
2. *Encryption and Control Keys*
3. *Challenge and Verify*
4. *Update Continuously*
5. *Readiness and Response*
6. *Exact and Specific Accountability Management*
7. *Control / Dual Controls*
8. *Layers*
9. *Awareness, Understanding and Testing*
10. *Monitoring*
11. *Principle of Least Privilege*
12. *Secure Removal and Deletion of Data*

While we won't cover all twelve principles in this eBook, we will highlight a couple below:

SPEED MATTERS: *As many treasury and finance professionals try to prioritize their fraud policies, they focus heavily on preventative measures to the exclusion of controls that would help identify fraud quickly once it has occurred. Even after the money has left the bank, however, speed matters. The more rapidly the fraud is identified, the more likely it is that some or all the money can be recovered with a subsequent rapid response. Controls such as reconciliation are often neglected because they are not seen as helpful in preventing a loss. In reality, however, same-day reconciliation can help you recover funds and, in some cases, actually can help prevent fraud. (For more details on reconciliation, see page 16.) The same goes for new technology, such as AI fraud detection, that are set to play an increasingly important role for TMS solutions.*

PRINCIPLE OF LEAST PRIVILEGE: *This principle is less well known than Segregation of Duties and is understandably less systematically enforced by many. Least privilege refers to giving people or IDs access exclusively to the information and functions they require. More access can be granted on an as-needed basis, but at all times, every user of a system has no more access than necessary. This not only minimizes the risk of an employee going "rogue" and being able to cause significant harm, but it also reduces the number of credentials a criminal can steal that would allow them the access they want. In a recent survey, use of the principle of least privilege correlated to 55% fewer losses or issues with ransomware, one of the fastest growing fraud types.*

> The more rapidly the fraud is identified, the more likely it is that some or all the money can be recovered with a subsequent rapid response.

Adding and Defending Layers

Another of the twelve principles is that of layering your security. To put it one way, the more layers of defense you have, the less likely it is that an attack can make it through all of them. Put another way, payment processes always have multiple layers to them already, and since each layer can be compromised, each layer requires protection.

The Human Element

There is a strong emphasis in modern treasury on technology, and for good reason. Technology is constantly changing and its applications within finance morphing, making it an important element for treasury professionals to study and understand. Additionally, cybersecurity logically emphasizes technology since its focus is on the ways our technology can be compromised and on technological defense.

However, every computer system has a user, or more often, a host of users. People are some of the most frequently compromised elements in a payment process, but they are also some of the most capable defenders if they have been properly trained.

This dramatic impact—whether positive or negative—that staff and their training can have on security outcomes appeared in a recent survey on Treasury, Fraud and Controls. According to the survey data, employee training correlated to lower loss rates related to various types of fraud. Firms that did not train their employees on payment fraud, security and cyberfraud saw the following ratios of increased loss:

- 1.5X Payment Diversion Fraud
- 2X ACH Fraud
- 2.5X System Level Fraud *(System Takeover)*
- 4X Business Email Compromise
- 4X Bank Mandate Fraud
- 5X Cyberfraud/Malware
- 5X Ransomware

While correlation does not always indicate causation, these statistics are interesting and should encourage treasury professionals to assess their staff training policies, especially given the rapid growth of attempts, success rates and loss levels for several of the fraud types listed.

It's highly recommended that firms require training at least annually for anyone involved in the payment process and that a testing component be included in this training. Employees need to know how to recognize a BEC message in their inbox, have awareness of the newest methods criminals will use against them, and understand the importance and the company policies regarding challenging and confirming a suspicious payment request—even if it appears to come from the CEO or CFO. Making sure staff has sufficient training on these issues can deeply strengthen one of the most vulnerable layers of the payment process.

Perimeter

The second layer of vulnerability and defense is the perimeter. This term refers to the access points and defense measures surrounding the data and systems. It includes elements such as hardware, firewall and user access.

Treasury has little involvement in setting up and maintaining the perimeter in most organizations. The setting up of routers, firewalls and user logins falls instead to IT. However, this is an area where the treasurer's proper role is that of "superintendent." The treasurer does not set up the routers or create new logins when a new hire is onboarded. Still, since it is treasury's job to make sure payment processes are secure throughout the organization, it is entirely appropriate to ask questions about how these tasks are being performed. The treasurer needs to know what is going on and how processes are working.

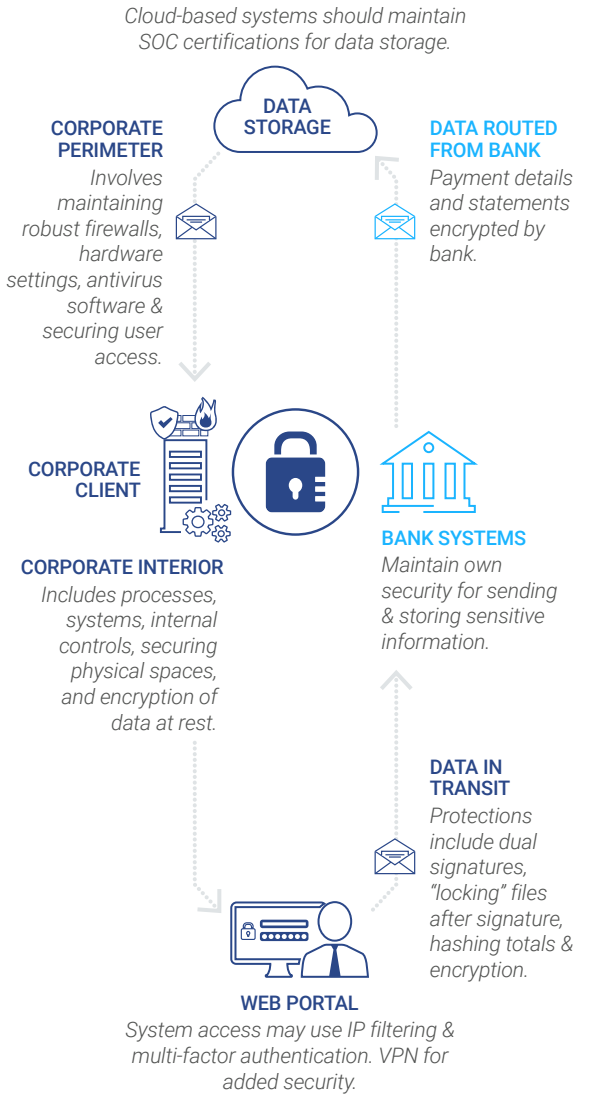
If your questions meet with vague responses such as, "It's locked down," it is also appropriate to dig deeper and ask what exactly that means, what steps are being taken, or who does have access. (The full meaning and implications of this role will be discussed in a later section on *page 17*.)

Interior

Within the perimeter lies the interior, a layer that includes processes, systems and internal controls. There are many questions for treasury to ask at this level, some of which will be directed inward at treasury itself, while many others will be directed outward again.

Elements and controls to assess within the interior include directory access, data encryption at rest, permission and audit trails, desktop security and desktop hygiene, as well as behavioral monitoring. While many of the controls needed for the interior are familiar to most, they can be neglected or bypassed by staff. Treasury should make sure not only that these controls are theoretically in place, but also that they are being upheld by regular checking, training and testing.

TREASURY TECHNOLOGY SECURITY COMPONENTS



Treasury's Own Framework

While many elements of the perimeter and interior are not directly related to treasury, a few areas of vulnerability and necessary control do fall within treasury's role. For these, treasury is not only the superintendent, but also the active party performing the work. To ensure proper handling of these issues, treasury needs to have their own security framework outlining the management of their own vulnerabilities and controls.

Access Points: The "Gates"

If we wanted to make our data and funds impossible for anyone to access, fraud prevention would not be nearly so much of a problem, but this would also defeat the purpose. We need sensitive information and funding to be accessible to the right people, and this requires building "gates" in the perimeter and in the smaller interior walls.

These gates become the most difficult points to defend. As treasury looks to confirm the security of its own systems, and the data and workflows for which it is directly responsible, access points should be prioritized. Wherever doors and gates are, "dirt" is liable to get in, and intruders will try the doors and windows long before they bother attempting to get through the walls.

In treasury, these access points include elements such as the department's network, directory, systems, the custody of credentials, and even elements such as the physical door and access to paper documents. All of these "gates" require locks and the discipline to keep the locks engaged.

Preferably, every access point should have more than one lock. The most crucial aspect of these locks, however, is that they are effective in their job of keeping people out. Many organizations take comfort in having a great number of controls – none of which are enforced. If you put three locks on a door, but two of them always have a key left in them, you effectively have only one lock.

Many, if not quite all, of the controls discussed below zero in on the defense of some of the most vulnerable access points, but there are many more. Take the time to review handoff points between systems, whether internal or external, and access points to your treasury department's office space, networks, directory, systems and so on. They will vary from company to company and department to department, so it's important that you consider your own unique gates, test the locks and add functioning locks as necessary.

Bank Account Management

One of treasury's most security sensitive areas of responsibility is bank account management. Every bank account and every signer constitute points of exposure, and yet many organizations fail even to keep track of them. Treasury's framework for security must include thorough bank account management. Accounts, activity, signers, controls in place (account level controls such as debit filters, vendor verification based on allow and block lists) and banking services (e.g., electronic preauthorization) should all be tracked. Monitoring these elements makes it much easier to notice fraudulent activity.

Account Architecture

Even with good bank account management, it can be difficult to keep track of every account's activity and that activity's appropriateness when the structure of those accounts is random. Organizing your accounts with intentional architecture designed to maintain clarity and efficiency is an important piece of treasury's framework. The most common and recommended basic architecture involves the use of a concentration account (also called a header account). In this model, funds flow into the collection accounts, flow from there into the concentration account, and from there are transferred out to the disbursement accounts.

> Every bank account and every signer constitute points of exposure, and yet many organizations fail even to keep track of them.

This separation, with all accounts being exclusively either collection or disbursement except the single concentration account, allows you to easily see your net for the day and to rapidly identify anomalies. If funds are disbursed from a collection account, for example, it's immediately clear that investigation is necessary.

Further categorization of accounts can prove helpful as well. Perhaps one account is exclusively used for ACH disbursements, and another is used for checks. With increased categorization comes increased ease of identifying an unintended transaction. In addition, when something in the day's totals is not as expected, the culprit transaction can be tracked down more easily when accounts are rigorously categorized.

Account and Transaction-Level Controls

Account-level controls and transaction-level controls overlap each other significantly, but it is helpful to consider controls from both perspectives. Also, note that an organized account architecture is complementary to account level controls. Since many of these controls rely on restricting the types of transactions allowed to pass through an account, they apply more readily when accounts are organized such that only one or two types of transactions should occur in each one.

Technology can also be a means of creating centralized directories that all payments leaving a company are checked against. Other controls rely on restricting the types of transactions allowed to pass through an account.

Allow Lists: Allow lists enable you to create a centralized database of beneficiaries and accounts that have been verified and that payments may be made to. Payments to beneficiaries or accounts not on this list can be blocked until approved manually and/or flagged by the system. This provides you with an additional level of security.

Block Lists: Conversely, you can also create a centralized database of beneficiaries and accounts that have not yet been verified and should not be used until further notice. Again, the system will flag or block these payments and you can intervene—either to stop the payment or to add the account in question to your database.

Debit Filters: Similarly, debit filters restrict the types of debits that are allowed in an account. For example, a debit filter might be set to block all ACH debits in an account intended for use exclusively with checks, or vice versa. A debit filter is primarily an account-level control.

Debit Blocks: While a debit filter restricts the types of externally originated debits that are allowed on an account, a debit block restricts disbursement activity in an account exclusively to internally originated transactions, blocking all types of debits that originate externally. This, too, is an account-level control.

Positive Pay: Positive pay is primarily a security feature for check disbursements with a control function at both the account level (the service is required and ensures all checks being presented for payment have been issued by the paying organization) and at the transaction level (each payment has its own individual record). With positive pay, transaction information on the issued checks is given by the account owner to the bank ahead of time, and the bank only processes the transaction if the data the payee presents matches exactly. Payee Match Positive Payment is an expansion on the traditional Positive Pay services, adding a matching requirement on the payee name, not just on the check number and amount of the payment.

ACH Positive Payment/Electronic Pre-Authorization: Various bank services allow certain entities to debit a bank account using EFTs. These services may have distinctions for individual entities (any amount), individual entities and amounts limits, or even individual payments. These, too, represent a combination of account-level and transaction-level controls.

Reconciliation: As noted in the 12 Principles, speed matters. Daily reconciliation is a highly recommended account-level and transaction-level control that helps identify account probing activities, unauthorized transactions, and errors by rapidly detecting problems while there may still be a chance of recovering funds or stopping the fraud while it is in flight. Reconciliation must be careful and thorough, however, especially in order to catch the probing that occurs prior to fraud. Since criminals often test an account by pulling out and then returning very small sums, sometimes less than a dollar, these transactions net zero and are easy to ignore. However, those responsible for reconciliation in your organization must be made aware that such transactions require investigation to ensure they do not indicate fraudulent probing.

Automated Detection Processes: Automated detection processes also play a role here. Moving forward, new technologies such as AI-driven fraud detection will become increasingly important and bring about more efficient security.

> The treasurer is responsible for ensuring the organization's payment security is effective and comprehensive even though many of the tasks involved fall outside his or her jurisdiction.

The Superintendent of Payment Security

We began this eBook by discussing the treasurer's role as superintendent of payment security. As a superintendent is responsible for ensuring a safe and effective learning environment even though they do not perform many of the duties they oversee, the treasurer is responsible for ensuring the organization's payment security is effective and comprehensive even though many of the tasks involved fall outside his or her jurisdiction.

This can be easier said than done, however. Below, we'll discuss some guidelines for most effectively validating the security of your organization's payment processes and fulfilling the role of superintendent of payment security.

Assess | Inquire | Direct

Assess:

In order to keep watch over the activities of the school, the superintendent must understand many things. He must know who is responsible for what, what the current state of the school is and what elements—whether external or internal—threaten the school.

Similarly, treasury must understand its own organization and the other departments and people involved in the payments process. What is IT responsible for? Which departments process what types of payments? Who is in charge of the security procedures for cross-departmental payment processes? Are the process steps and points of exposure clearly inventoried? What remediation steps are in place to counter known weaknesses?

In addition, treasury must understand the current threats and risks to payment security. With criminals constantly adapting their methods, and security standards and leading practices adjusting in response, the treasurer must put in the effort to stay current on developments in the payments, fraud and security landscape. Combining this internal and external knowledge, the treasurer must also realize how his or her organization stacks up against similar groups and relevant standards.

Developing this level of understanding helps treasury identify the surface areas of exposure in the organization. The next step is to check in on those responsible for various areas and ensure that exposed surfaces are adequately protected.

> For the most part, the superintendent of payment security performs his duties by talking to those responsible for various payment-related areas and asking many questions.

Inquire:

Treasury cannot and should not spend all their time looking over the shoulders of other departments and watching their every move. This is not what we mean by supervision or oversight. For the most part, the superintendent of payment security performs his duties by talking to those responsible for various payment-related areas and asking many questions.

It is appropriate for the treasurer to probe rather deeply with these questions. When questions meet with surface-level answers, such as, "Yes, that process is secure," or "Absolutely, that access is locked down," treasury can ask follow-up questions to find out what is meant. "Locked down," for example, might still mean that the entirety of IT has administrative access, which is not in line with the principle of least privilege.

The intent, however, is not to make others uncomfortable so much as to gain understanding and probe out areas that others may not have thought of. Treasury should enter these discussions for the sake of understanding what others are doing, how exactly they are doing it and why. While maintaining an uncompromising stance on vigilant security, the treasurer should take care to hear out and discuss the concerns and thoughts of others.

Direct:

Having listened carefully and assessed the situation, treasury's next step as superintendent is to direct. Work alongside the CISO and others. Communicate to the various departments involved in payments what they need to do to bring security to the proper level. While micromanaging should be avoided, this direction may appropriately involve specifying certain controls that need to be implemented.

Fraud in Action: Three Examples

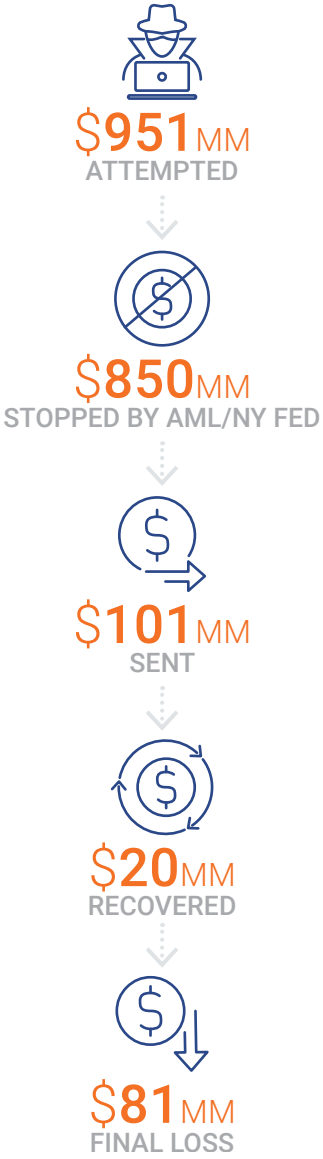
After discussing the theories of fraud and security for some time, it can be helpful to review some real events, their causes and their fallouts. This can help build our understanding of the wide range of attack methods, the ways common controls can be bypassed and breached, and the angles (both external and internal) from which fraud can originate.

Central Bank of Bangladesh: System-Level Fraud

- **WHAT HAPPENED:** *In early 2016, criminals sent wire transfer requests totaling $951,000,000 to the Central Bank of Bangladesh, $101,000,000 of which was sent out before anti-money-laundering controls were tripped at the Federal Reserve Bank of New York. A little over $20,000,000 was recovered due to a spelling error, but the remaining $81,000,000 was permanently lost. The head of the bank was forced to resign a year prior to his intended retirement.*

- **FAILURES OF DEFENSE:** *The Central Bank of Bangladesh didn't have firewalls up at every access point. This made it a particularly easy target. Its office routers were bought used, so they were not up-to-date, and they were left on the default security settings. In addition, system doors had been opened during testing and implementation and had not been locked down again when the system went into production. As for notification controls, the system would print off a notification whenever a payment was made, but the criminals successfully hacked the notification system, preventing any of the necessary alerts from printing. Finally, the bank failed to notify the governing authorities of the fraud in a timely manner. This delay compounded an already bad situation, making their attempts to recover funds even more difficult.*

- **FRAUD METHODS:** *In this system-level fraud, the criminals studied their victim ahead of time, took advantage of vulnerabilities and were able to compromise passwords, codes and cryptographic keys. They also took advantage of the weekend, which gave them until Monday morning to move the funds.*



Australian Shipping Company, Toll: Ransomware

- **WHAT HAPPENED:** *The global delivery and transport company Toll, headquartered in Australia, was a victim of ransomware twice in early 2020. In January, Toll was hit with ransomware, impacting over 1,000 of the company's servers. In May of 2020, the company was hit by ransomware yet again. While Toll refused to pay the ransom, the attacks caused delays and disruptions for customers, who used social media to raise concerns, a detrimental blow to the company's reputation.*

- **FAILURES OF DEFENSE:** *While Toll did not disclose what vulnerabilities were exploited by the attacks, the hackers seemed to indicate that the vulnerabilities that allowed Toll to be breached the first time were not repaired or adequately bolstered afterwards, leaving them open to the second attack.*

- **FRAUD METHODS:** *The attacks used Ransomware-as-a-Service, a model in which an illegitimate business sells ransomware to individuals or groups. The type of ransomware involved in Toll's first attack was Netwalker, also called Mailto, which was first noted in August 2019. The second attack used Nefilim ransomware.*

Wirecard: Internal Fraud

- **WHAT HAPPENED:** *In June of 2020, Ernst & Young refused to sign off on Wirecard's financial statements, as their audit showed €1.9B ($2.1B USD) missing. This amount, which was nearly half the balance sheet, was soon determined to have never existed. In response to the announcement of the missing funds, Wirecard faced rapid and devastating devaluation—dropping over 60% in value in a single day—and declared bankruptcy. The CEO resigned and was arrested a few days later.*

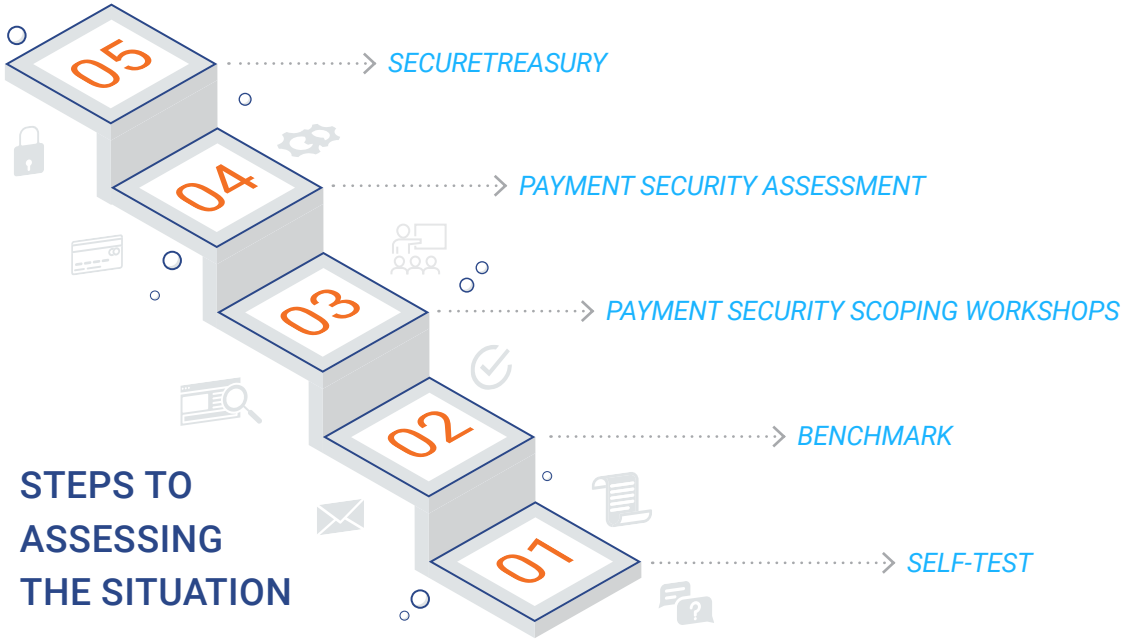
- **FAILURES OF DEFENSE:** *Wirecard's internal controls proved insufficient or faulty, given that it appears several parties were creating fictitious activity. While discussions about failures of the external auditors is appropriate, internal controls can't be sidelined. Proper bank account management alone—including elements such as daily visibility, automated reconciliations, automated cash posting segregation, and treasury running its own bank account audits on signers and accounts—should have made the 'missing' cash and fraudulent activity far more noticeable and the fraud easier to detect.*

- **FRAUD METHODS:** *While investigations continue at the time of this eBook's writing, we currently know that Wirecard falsified their financial statements, inflating revenue and overstating cash approximately twofold. The Financial Times had previously accused Wirecard of roundtripping, also referred to as "Lazy Susans"—selling and buying back the same or similar assets to increase "noise" and inflate the appearance of growth and financial activity. Collusion is suspected among high-level officers, some of whom are being charged or sought. It is also known that short-sellers had been betting against the firm to affect stock prices for years.*

An Initial Roadmap and Resources

> When it comes to fraud, those at the back of the pack, so to speak, are the most likely to become victims, and as rapidly as the payments and fraud landscapes change, it can be surprisingly easy to fall behind.

The constantly changing threats of fraud, the various fronts on which it can attack (both internal and external) and the vast undertaking of shoring up organizational defenses can leave treasury struggling to know where to start. In the following section, we will outline a roadmap for getting started in assessing your current level of organizational security and identifying the areas that most urgently need tighter defenses. Included is information about five resources you may wish to use as you strengthen various aspects of your payment security. These services and subscriptions individually provide various levels of review or control, and they offer a more comprehensive defensive posture if used together.



Assessing the Situation

The first step in bolstering security is identifying your current situation. How well is your organization prepared for various types of attacks? How good are your defenses? How do you know? Starting by asking yourself some thought-provoking questions and doing the research to uncover realistic answers can help you gain a basic understanding of your company's current state and most urgent needs.

Resource 1 – Self-Test

Link Here. This free resource consists of a battery of eight questions that lead you through a basic evaluation of your organization. At the end of these eight questions, you receive an overall indicative score.

This exercise is similar to getting your vitals checked. It gives a basic indication of the organization's overall health and shows when a certain area needs further investigation. The scope of this test is broader than security alone, but security is an important component measured.

Resource 2 – Benchmark

When it comes to fraud, those at the back of the pack, so to speak, are the most likely to become victims, and as rapidly as the payments and fraud landscapes change, it can be surprisingly easy to fall behind. Recognizing how you measure up against similar companies shows you where you may be putting yourself at significant risk by falling behind. While taking your vitals with the self-test is free, benchmarking is a low-cost, more in-depth way to gather insight on your company's current situation and most urgent security risks.

Our benchmarking services begin by having you respond to a battery of questions regarding your practices and plans, including payment security. We then compare those responses against the broader market, making sure the comparison is always between companies of similar size and complexity. The payment security benchmark report also provides information on what organizations ought to be doing to meet current leading practices and standards. This offers you an excellent starting point, showing your gaps and the areas that need attention.

Resource 3 – Payments Security Scoping Workshops

The first step to achieving a more secure payments setup must be an audit of all the processes, workflows, technologies and stakeholders currently in place. You need to know where you're coming from to know where you can and should go. However, we've seen that payments security is multi-faceted, and while treasurers act as "superintendents," they cannot be expected to deal with all of these aspects on their own. That's why Coupa offers extensive payments security scoping workshops, including remote workshops, conducted by experienced treasury experts intricately familiar with treasury technology. Experts guide treasurers through the assessment of their existing payments security landscape and help them map out a future state as well as very practical, actionable steps to get there. This way, you achieve a much more secure setup that reflects the needs but also the vulnerabilities of your specific company and brings you lasting peace of mind.

Resource 4 – Payment Security Assessment

This Strategic Treasurer service is another option for conducting a security audit. It entails a custom review of your organization's payment processes by a team of experienced treasury consultants. The review usually spans from origination of vendor payee setup, to payment origination, to delivery and confirmation of payment information to the financial institutions. This thorough, objective, expert feedback on your specific situation can dramatically raise your levels of security, identify and protect small but dangerous exposures, and help you realistically and efficiently reach the standard of good corporate conduct your organization needs. For less complex organizations, there are two assessment levels. For larger organizations and those that are particularly payment intensive, a custom proposal for the assessment is provided.

Resource 5 – SecureTreasury

Earlier in this eBook, we discussed the importance of the human element and showed how employee training on payments, fraud and controls correlates to dramatically lower rates of fraud loss. SecureTreasury is an online training program with testing, focused on payments and treasury. As a subscription-based program that adds and updates courses over time, SecureTreasury offers companies a way to keep their employees current on developing fraud issues and to repeat training on an annual basis, as is strongly recommended. The program includes multiple courses and distinct classes which can be taken as needed based on an individuals' responsibilities and role within your organization.

Where to Learn More

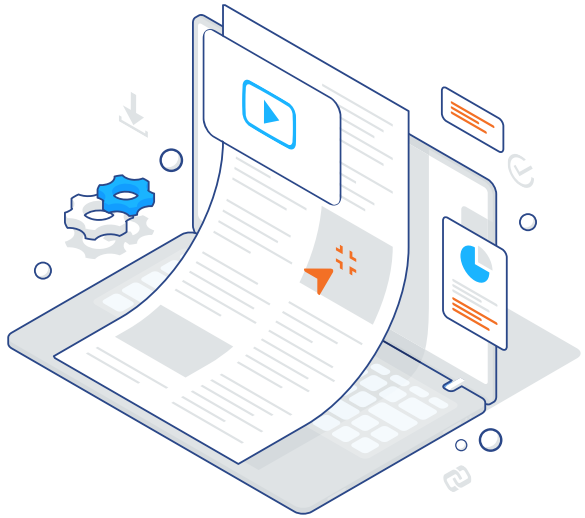
Hopefully this eBook has proven valuable to you as a starting point and foundation for strengthening your organization's stance against payment fraud. To learn more, we recommend the following resources:

- *Fraud Week YouTube Videos* - These brief videos (all well under five minutes) explain various principles of payment security and cover additional case studies of fraud.

Webinars – For more thorough discussion of various topics, watch the replays of these webinars, as well as others on our website:

- *Treasury Fraud and Controls: 2020 Survey Results*
- *The Why and How of Securing Treasury and Payments*
- *Security Challenges with Payments*
- *Fraud Is Rampant: Six Key Principles for Security*
- *Combatting Fraud: Six More Principles for Security*

Internet Crime Complaint Center – The FBI's IC3 site is full of valuable information on current threats, with consumer alerts, industry alerts and annual reports.



Eight Actions to Consider

Each of the following actions are highly recommended. Implementing even one of these can significantly bolster your stance against fraud and can open the door for future security improvements as well.

#1. ***Create a comprehensive inventory of payment paths:*** This is one of the first steps in assessing payment security. Make a list of every single payment path running through your organization, no matter how small or obscure.

#2. ***Identify top problems with each payment stream:*** A logical follow-up to the inventory, this action shows you areas where you are most likely to be exploited so you can shore up the defenses.

#3. ***Benchmark your security at least every other year:*** When it comes to payment security, what was paranoid last year may be standard now, and falling behind your peers makes you an easy target.

#4. ***Assign specific responsibility for monitoring fraud types in the news:*** To stay ahead of the criminals, you need to watch their movements carefully. To make sure that happens and to simplify the matter, divide and assign the monitoring of developments in various fraud types among treasury staff.

#5. ***No less than quarterly, hold a fraud and control briefing with your full staff:*** A quarterly meeting, if not a more frequent one, focused on security helps staff keep each other informed and provides a space for discussing vulnerabilities and potential solutions.

#6. ***Be intentional about research and learning:*** Every month, listen to a podcast, watch a webinar, read an article, or learn by whatever means suit you. Whatever you choose to do, be intentional.

#7. ***Get payment security specific training:*** While general training on security can be quite helpful, a good training course specifically for securing payment processes pinpoints the unique challenges you need to know about and shows you how to address your organization's most pressing payment security needs.

#8. ***Consider technological support:*** Take the opportunity to familiarize yourself about what a treasury management system with integrated controls, secure payment gateway, and other fraud prevention technology can offer.

Get actionable "this is what you can do right now" advice:
Click here.

For general information, email us at: *info@strategictreasurer.com*

About the Firms

Coupa and Coupa Treasury

Coupa empowers companies around the world with the visibility and control they need to spend smarter and safer. By breaking down silos and unifying the procure to pay process, Coupa provides greater visibility, control, and scalability of payments, working capital and treasury. Coupa Treasury helps businesses to optimize liquidity and spend by achieving greater visibility and transparency, increasing agility and improving forecasting and planning. Businesses are empowered to improve operational performance with automation across multiple subsidiaries, currencies, accounts and users and to mitigate security, compliance and liquidity risk. To learn more about Coupa, visit *www.coupa.com.* Read more on the *Coupa Blog* or follow *@Coupa* on Twitter.

coupa.com

Strategic Treasurer

Strategic Treasurer provides consulting, research, and professional services for treasury management, security, technology, and compliance. Since 2004, corporate clients, banks, and fintech providers throughout the world have relied on their advisory services which are backed by a deep awareness of current practices, plans, and perceptions through their annual surveys and decades of treasury experience.

The mission of Strategic Treasurer is to elevate and enhance the practice of treasury by advising individual clients and informing the industry at large. Headquartered in Atlanta with consultants based out of Philadelphia, Cleveland, and Washington DC, Strategic Treasurer guides treasury and finance professionals through real-world, mission-critical issues that organizations face today.

STRATEGIC TREASURER

+1 678.466.2220
strategictreasurer.com
info@strategictreasurer.com

coupa

coupa.com

Strategic Treasurer

strategictreasurer.com