Protecting from Fraud

Understanding and Attacking the Key Sources of Fraud

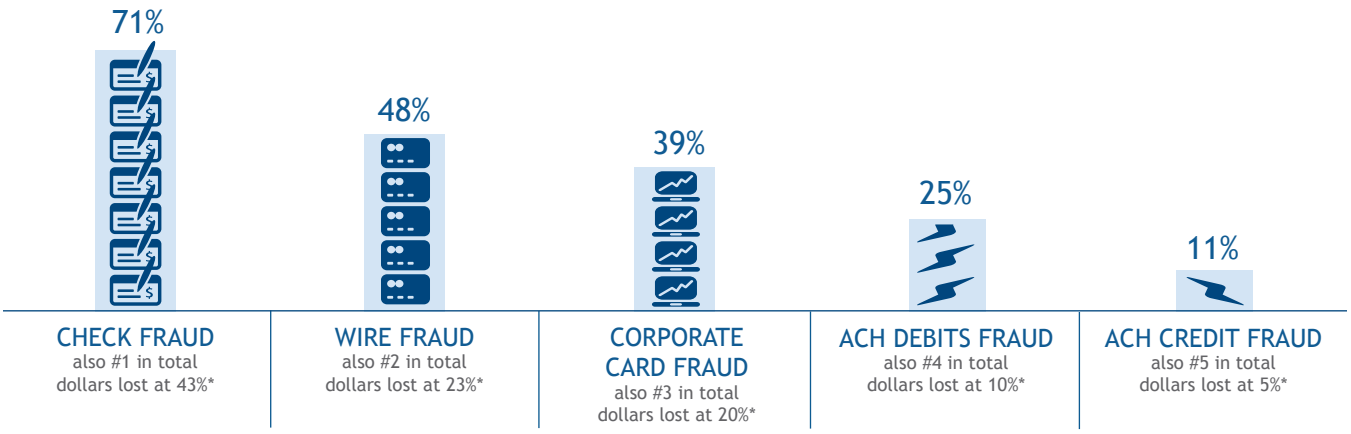
Fraud prevention has a significant role in payments strategy. Fraud based on paper-driven processes and checks continues to be the number one form of payment fraud perpetrated on businesses. Criminals have adapted and have found new ways to exploit system weaknesses with advanced phishing schemes, business email compromise, and other emerging fraud plots. Understanding the types of fraud afoot, the risks involved and the best prevention measures has never been more important.

At SunTrust, we want to help you understand how electronic payments can prevent and mitigate the impact of fraud. The SunTrust OneTeam Approach℠ brings an integrated team with the right financial and industry expertise from across our organization to help our clients pursue the best financial strategies for their businesses. Our latest research highlights *Directing Payments*, *Managing Collections*, *Protecting from Fraud* and *Reporting and Controlling Cash*. SunTrust and industry experts discuss linking your business plans, your capital requirements, and your payments strategies to generate smart growth.

Understanding Payment Fraud and its Prevention

Sources of Fraud by Payment Method

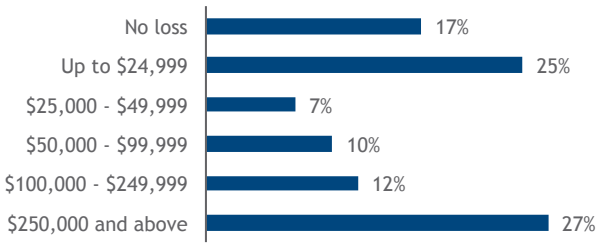
(% of organizations that experienced attempted or actual payments fraud)



* Percentage distribution of organizations that experienced payments fraud
Source: AFP Payments Fraud and Control Survey, 2016

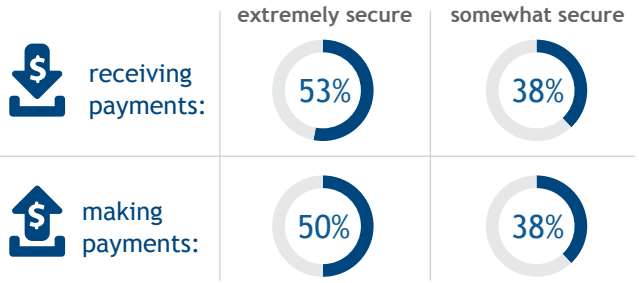
Losses when Fraud Strikes

(% distribution of organizations that experienced payments fraud)



Source: AFP Payments Fraud and Control Survey, 2016

Business Owners Felt Secure About Electronic Payments



Source: SunTrust Research

SunTrust

Fraud by the Numbers

Businesses of all sizes are at risk for fraudulent activity, especially when their cash flow relies on paper payments. The 2016 AFP (Association of Financial Professionals — http://www.AFPonline.org/fraud) Payments Fraud and Control Survey found that 73% of organizations have experienced actual or attempted fraud. Paper checks are the target 71% of the time in these fraud attempts, and of those companies that had attempts, 28% suffered a loss and half of those losses were less than $25,000 ("Fraud", AFP, 2016).

Paper is not the only target. Wire fraud was the second most frequently cited fraud target and increased 80% since 2015. Credit and debit cards were the third highest fraud source. As the face of fraud continues to change and seeks new weaknesses in the payments system, SunTrust and AFP executives share their views on the best ways to protect your company.

Trends and predictions

"Fraud has risen in the past year with 73% of businesses subjected to attempted or actual fraud, up from 62% in 2014," says Magnus Carlsson, Manager of Treasury and Payments at the AFP.

Robert Blair who heads Product & Digital for Treasury & Payments Solutions at SunTrust adds: "Every day, there are people around the world whose full-time job is to figure out ways to rip off businesses and consumers. They are remarkably intelligent. Instead of going to work in programming for a company, these thieves are programming and attacking our systems or are hacking, creating bugs, etc. As soon as we squash one, they've got another. It is rampant."

While the larger fraud incidents still make the headlines, the gap between fraud attempts at larger versus smaller organizations is shrinking. "Now in 2015, the companies with under $1 billion in revenue are just 2 percentage points lower on fraud attempts than larger ones," Mr. Carlsson notes ("Fraud", AFP, 2016).

There are a broad range of fraud schemes hatched towards Middle Market companies and Small Businesses. Mr. Carlsson notes, "Fifty percent of companies reported attempted or actual fraud from a technique called business email compromise. This fraudulent email tries to mimic the language and tone of a senior executive asking a company subordinate to wire funds to the criminals. AFP is supporting the FBI in understanding this crime and the best defenses to prevent it."

Using technology to your advantage

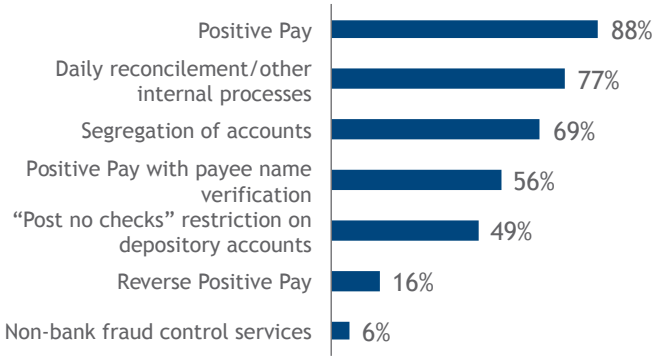
There are many ways to combat fraud — from simple to complex. Advancing technologies improve the success of fraud attempts; however, your company can also use that same technology to your advantage to thwart these attacks. Solutions range from simple process changes to improving your electronic processing and reconciliation capabilities.

"From a process perspective, simple solutions such as segregation of duties, dual payment approvals and quickly reconciling accounts all help fight fraudulent activities," says Carolyn Pyle-Kennedy, manager of Technical Product Consulting for SunTrust Treasury & Payment Solutions. "Another area for fraud protection improvement is vendor on-boarding and compliance. Many large companies have large number of business partners with close strategic and operational ties. Ensuring that partners have business practices that match those of your company, planning how they will technically connect to your company and ensuring that they have adequate security when handling your business can be a critical safeguard." Some of the larger credit card breaches — Target and Home Depot most recently — can be traced back to lack of security on the part of a new vendor.

Michael Maza, head of SunTrust Treasury & Payment Solutions adds, "Helping our clients reduce or eliminate the risk of a financial loss due to fraud is paramount. Our solutions incorporate preventive measures such as account monitoring, identification of suspicious items, and alerts to the client to make decisions on questionable transactions. The best defense is always a great offense, so we strive to detect potential fraud before it occurs."

Check Fraud Prevention Measures

(% of organizations that experienced at least one attempted check fraud)



Source: AFP Payments Fraud and Control Survey, 2016

SUNTRUST

Phishing 2.0

Phishing's most common form — fraudulent messages requesting bank, PayPal or account information — continues to permeate the Internet. Websites storing financial information regularly warn customers not to respond to unsolicited emails. With the effectiveness of these fraudulent emails being slowly diminished by education and junk/spam email blocking, a new version of phishing, 2.0, has emerged with a number of new schemes:

Business Email Compromise (BEC) — One of the most prevalent new schemes is the spoofed email. Companies are targeted by sophisticated criminals who have hacked into the business email system and studied top executive email behavior. With access to company directories, online calendars, and email schedules, these fraudsters create an email that closely mimics the language and speaking style of the executive. They then send an email instructing a subordinate to wire transfer money to a certain account — at a time when the "real" executive is in a meeting, traveling or simply unable to be contacted to confirm the instructions. If there are no checks and balances or requirements to double check wire transfer requests, the subordinate wires the money to the requested account, and the money is lost.

Smishing — Short for SMS phishing, smishing involves tricking a mobile phone user into downloading a Trojan horse virus or other malware onto a device.

Twishing — Twitter phishing is an attempt to induce people to click a link that appears to be the Twitter home page. The user then enters her login data, which gives fraudsters access to her Twitter page and other internet sites.

Ransomware is a threat posed when a user unsuspectingly downloads an infected email attachment or visits a compromised website. The downloaded malware either locks up the system, or encrypts it, and then demands payment in order to release the data. Originally much more prevalent for consumers, sophisticated Ransomware schemes are increasingly targeting government entities and commercial businesses, asking for more lucrative payouts to release the captive data.

Fake Mobile Apps are becoming prevalent as the world becomes more connected with mobile devices. A recent rash of fake mobile apps, including fake CNN, BBC, Facebook Messenger, and WhatsApp applications, have made the rounds through mobile devices. Primarily aimed at luring users to ads and adware, these apps also collect data about their users which could be put to further fraud use.

"Despite the continuing drop in the number of checks, check fraud is still number one in terms of fraud," says Mr. Carlsson. Increasing your company's penetration of electronic payments and collections can be a huge asset in combating fraud. The first step involves reducing the opportunity for fraud while still dealing with paper payments by separating duties, reconciling accounts daily and using Positive Pay services for all paper checks. The next step involves accepting and making more payments electronically with less opportunity for human intervention in the process. Finally, implementing checks and balances on electronic debits from your accounts with restrictions and controls will lessen the risk of fraud.

"Many CFOs realize that they can mitigate paper payment risks as well as electronic fraud with a series of basic controls, such as automatic reconciliation of accounts, blocks, and filters on ACH payments or instituting UPIC," emphasizes Ms. Pyle-Kennedy.

As the paper check becomes less and less used (paper check volume is going down 6% per annum), the majority of fraud attempts will turn to electronic methods (The 2013 Federal Reserve Payments Study, 2014). Fortunately, electronic payments are more complex and require greater sophistication to commit fraud. Additionally, businesses have the tools today to turn technology against potential fraudsters and stay safe from fraud.

SunTrust

Who Owns the Fraud Problem?

Fraud costs the nation in excess of $3 billion per year, with banking having one of the greatest number of cases reported (ACFE, 2014). General public perception is that detection and addressing instances of fraud is a financial industry problem. While this may be true for some types of white collar crime, the situation is far more complex.

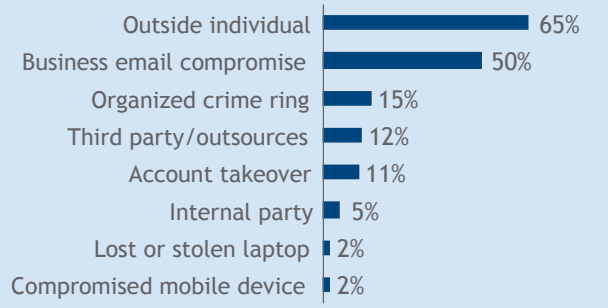
Types of fraud

Fraud comes from many sources, some internal and some external to the banking customer. While internal fraud has been around for a long time and requires continuous vigilance, external fraud is a growing problem.

Where are the Criminals?

So where is this fraud coming from? Most of it is from outside the organization:

(% of organizations that experienced attempted or actual payments fraud)



Source: AFP Payments Fraud and Control Survey, 2016

Internal (occupational) fraud

Internal fraud is typically a single individual or several working in collusion to exploit vulnerabilities available to them through employee access. This type of fraud is addressed by businesses setting up procedures and controls like division of duties and approvals for transactions. According to David Sawyer, a Certified Fraud Examiner and Partner at Frazier & Deeter, "Many organizations don't train managers or employees to understand why rules are put in place. Sometimes employees will over-ride policies and procedures that were put in place for a reason that they don't understand." Workers often just want to get the job done and may see protective procedures as barriers. One-time "workarounds" to circumvent these barriers can become business as usual over time, providing an opportunity for those who want to exploit them.

Responsibility for addressing internal fraud lies with management that set up the controls and training and with employees who must follow the procedures and work to the standards to which they have been trained. "Internal controls have to be embraced not only from the board room, but they have to extend all the way down to the mail room," says Sawyer.

External fraud

When a company or account is targeted by outside attackers, sensitive information can be accessed. This information can be used by the attackers to move funds directly or to exploit procedural weaknesses. An example of such an exploitation breach is hijacking the email system and sending a directive from the CEO's email address to move funds to a specified account via wire transfer.

One of the fastest-growing external threats is the use of Remote Access Trojans (RATs) to take over an otherwise legitimate computer inside the company's network and use that computer to access accounts just as the computer's legitimate user would. This can happen without the user ever knowing the software is there and is very hard to detect because the commands are coming from a legitimate computer. "Account takeover is one of the biggest areas of risk these days," says Sawyer.

Responsibility for external fraud can be hard to pinpoint. The business has a responsibility to set up procedures and controls to contain breaches, to review statements, and conduct reconciliations in order to detect problems as early as possible. In the case of a Remote Access Trojan attack, though, liability is often shared between a company and its bank. The bank can bear more responsibility for situations in which it is expected to have a high level of control such as properly handled Positive Pay and Reverse Positive Pay.

SunTrust

Trends in fraud

There are several trends in fraud that businesses should consider:

- **Rise in fraud during challenging economic times.** According to Sawyer, "When the economy is bad, people generally find a way to steal in order to supplement their income." This can increase both internal and external fraud globally, and represents a need for heightened vigilance even though the company may be under economic pressure at the same time.
- **Growth in cyber-fraud.** "Cyberthreat is one of the biggest emerging threats we see," says Sawyer. Hackers continue to test every aspect of technology, both internal to the bank and through its customers. "A lot of companies are taking out 'Cyber Threat Insurance' now to protect against these threats, a great recommendation for clients, provided that the company's procedures are also being addressed," says Sawyer.
- **Failure to monitor online transactions.** People rely more on systems and online information and tend to trust both. "In this day and age, many people are doing their banking online and they don't even look at their statements anymore, let alone do a bank reconciliation," says Sawyer. This trend towards not watching account activity and truing up balances provides an opportunity for those who wish to commit fraud.

Handling fraud

The first step in handling fraud is understanding the liability it represents. Caveat emptor ("let the buyer beware") applies to banking customers who have duties and responsibilities in detecting and dealing with many types of fraud. In some cases, the bank has no legal liability for fraud, particularly when it involves debit cards or the breakdown of a customer's internal controls.

Resistance to fighting fraud

Because the fight against fraud is ongoing, it may get lost in the "crisis of the moment." Particularly when the economy is not at full strength, banks and their customers may be so busy that they de-prioritize or mentally postpone the issue of fraud, thereby creating opportunities that can be exploited.

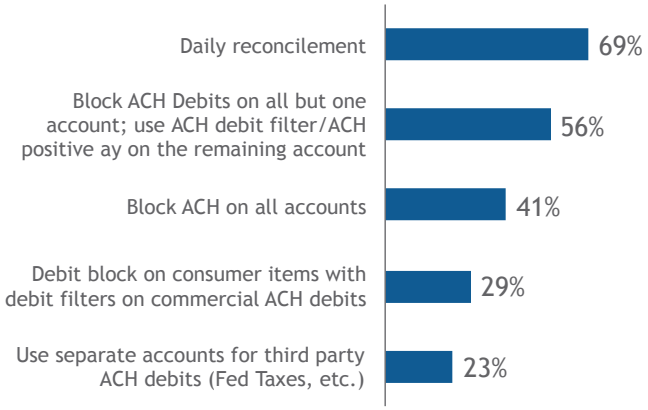
The assumption that fraud is someone else's responsibility — auditors, for instance — can prevent front-line managers from thinking much about the problem or being proactive against it.

Recipe for success

The fight against fraud is a team effort involving both the bank and its customers. "Everyone must take ownership and responsibility," says Sawyer. Any weakness can be exploited from within or without, so constant vigilance is necessary to keep fraud under control. This partnership means that anti-fraud efforts will continue to be a joint responsibility for the foreseeable future, and will depend on everyone involved in transactions to be informed and alert and to conform to well-thought-out controls and procedures.

ACH Fraud Prevention Measures

(% of organizations that experienced at least one attempted check fraud)



Source: AFP Payments Fraud and Control Survey, 2016

SunTrust

Customer Data Defrauded: How Breaches at Target and Home Depot are Shaping the Cyber-security Landscape

Two of the highest profile breaches have occurred at major retailers Target and Home Depot. Over 50 million customer records, including credit and debit card information as well as email addresses and phone numbers, were stolen in both incidents. Both companies are facing fallout from the breaches that could result in millions of dollars lost in the coming years. Understanding how these breaches happened and what we can expect can help business leaders protect their businesses from fraud.

The Target breach

Retailers with their large customer databases are a prime target for hackers looking for sensitive and valuable customer Payment Card Industry (PCI) information. While most retailers take security at the utmost importance, there are flaws in the design of their internal systems that allow hackers inside firewalls or human error that allows phishing schemes to break into sensitive data. In fact, up to 80% of data breaches (USA Today, 2014) can be attributed to employee negligence — anything from employees leaving a server room door open to giving out their passwords.

One of the highest profile cases in recent years was the Target breach that occurred during 2013. On Black Friday, more than 70 million pieces of customer data including credit card numbers, addresses, and phone numbers were stolen. This breach was enacted through malware installed on all U.S.-based checkout registers. As a result of these security failures, customer data was stolen and ultimately sent offshore to servers in Russia.

Less than six months prior to the breach, Target had spent $1.6 million on a malware detection tool to detect the very type of malware that ultimately caused the breach. Unfortunately the detection was ignored because of either a human error or a flawed procedure that interrupted the expected malware removal.

The initial point of entry for the hackers was through a third party vendor breach. Login credentials were stolen via a phishing email opened by an employee. These credentials were used to enter the Target intranet where PCI information was assumed to be walled off from other areas of the network.

Once into the vendor area, there were holes in the internal fire walls between the PCI information and vendor data area that hackers exploited. The result provided the opportunity to install the malware that collected the customer data.

Next up, Home Depot

Approximately a year after the Target breach, Home Depot experienced a startlingly similar breach through the company's self-checkout Point of Sale (POS) system. Hackers used stolen third party credentials to access the Home Depot network and exploited a vulnerability that allowed them access to the self-checkout system and the ability to install malware that collected customer card information. 7,500 Home Depot store self-checkout registers were targeted by the malware upload.

In the Home Depot breach, over 56 million customer debit and credit card numbers were stolen in addition to 53 million customer email addresses. The total monetary impact to the company is estimated to be nearly $10 billion incurred through loss of business, disruption in business operations, lawsuit settlements, and identity theft protection for customers.

Both Target and Home Depot have invested heavily in the new EMV chip-and-PIN technology that promises to help reduce the ability for hackers to access PCI information held by retailers in POS systems which have been the demonstrated weak point in data protection. While EMV chip adoption requirements implemented in 2015 will close the window on the Target and Home Depot fraud schemes, business leaders can expect fraud perpetrators to be searching for the next set of flaws that will yield them valuable personal data. Only time will tell where hackers will surface next, but data breaches continue to be at the forefront of cybersecurity evolution.

SunTrust

Limiting the Five Primary Fraud Threats

The threat of fraud in today's world is real, and few organizations are strangers to its effect. Every potential victim, i.e., every business, should take advantage of the tools at its disposal to stop fraud.

Account Fraud **THE THREAT:** **73% of organizations have experienced fraud** ("Fraud", AFP, 2016)	Solution	Online Courier
	How it provides fraud protection	Provides real-time notification of transaction and balance detail
	How it works	• Creation of online profiles allows selection of reports, alerts and desired format • Automatic "push" via FTP, PC download, dial-up or fax • Optional wireless alerts to smartphone
	What it solves	• View transaction detail for potential fraud detection • Monitor account balances for significant changes
Check Fraud **THE THREAT:** **#1 in fraud attempts. 71% of companies targeted noted check fraud; #1 in total dollars lost at 43%*** ("Fraud", AFP, 2016)	Solution	Positive Pay
	How it provides fraud protection	Flags discrepancies against company-supplied check-issued files to verify the authenticity of checks presented
	How it works	• Validates against issued date, check number and amount; verifies payee name • Provides automatic pay/return defaults
	What it solves	• Quickly identifies check fraud. reducing losses • Notifies of discrepancies through online banking • Provides for online banking pay or return decisions • Reduces staff workload
ACH Fraud **THE THREAT:** **25% of fraud was due to ACH debits; 11% due to ACH credits** ("Fraud", AFP, 2016)	Solution	ACH Fraud Control
	How it provides fraud protection	Places blocks and filters on all or specifically identified ACH transactions in designated accounts
	How it works	• Ability to block all debits, credits, or both • Approve/decline ACH transactions on occurrence date with Online ACH Control • Reporting via Online Courier each morning • Set up specific Standing Authorizations at the transaction level to allow for payments like Federal taxes, corporate healthcare and other self-insured payments managed by a third party
	What it solves	• Reduces losses and minimizes cost • Improves control over ACH transactions and enhances ACH usage • Minimizes cost
	Solution	UPIC — Universal Payment Identification Code
	How it provides fraud protection	Provides user with a universal routing transit number and a unique proxy account number that can be supplied to payers for incoming ACH payments
	How it works	• Bank issues a UPIC to relay to trading partners • Transactions using proxy account number automatically routed to correct account upon receipt of incoming ACH payments; systematically blocks debits
	What it solves	• Provides receivables alternative • Accommodates clients who want to remit payments electronically and provide payment data through EDI (Electronic Data Interchange) • No change in payment routines for trading partners • Blocks sensitive proprietary account information

* Percentage distribution of organizations that experienced payments fraud

SunTrust

Corporate Card Fraud

THE THREAT:

#3 in fraud attempts. 39% of companies targeted noted corporate card fraud; also #3 in total dollars lost at 20%*

("Fraud", AFP, 2016)

Solution	Enterprise Spend Platform
How it provides fraud protection	Provides a comprehensive online card management application for managing T&E, procurement and payables processes for Corporate and Purchasing cards.
How it works	• Enhanced reporting to: - Implement pre and post purchase controls - Audit spending - Manage program • Allows for: - Customizable business rules and work flow - Transactional review and "decisioning" - Electronic attachment of receipts/expense reports
What it solves	• Improved spending controls with online account monitoring • Increased control with built-in alerts, email rules and audit features • Online access to automatically activate/deactivate cards and raise/lower individual spending limits

Solution	ESP Express
How it provides fraud protection	Provides an easy-to-use online card management application for Commercial One Card
How it works	• View and manage cardholder detail and accounts • View both transaction detail and statements at the card level
What it solves	• Improved spending controls with online account monitoring • Online access to automatically activate/deactivate cards and raise/lower individual spending limits

Wire Fraud

THE THREAT:

#2 in fraud attempts. 48% of companies targeted noted wire fraud; also #2 in total dollars lost at 23%*

("Fraud", AFP, 2016)

Solution	Multi-level security controls
How it provides fraud protection	Execution through online banking provides for multiple levels in two ways: • Must match the authorities designated in writing and stored within the banks' Wire Facility • Requires Company and User ID, User Password for login • Requires Trusteer Rapport with keystroke encryption and malware deactivation • All wires require dual approval
How it works	• Wire transfer authorities are approved by the company's designee (account signer) and submitted to the Wire Facility • Wire transfer capability is set up through SunView giving access to approved initiators/approvers in accordance with the Wire Facility instructions
What it solves	• Reports are available in real time • Both incoming and outgoing wire information can be pushed to designated staff through Online Courier at pre-defined thresholds • Allows for the building of wire templates for repetitive wires, decreasing errors and fraud

* Percentage distribution of organizations that experienced payments fraud

SUNTRUST

Building an Electronic Payments Strategy

Payments strategy has a broad business reach, from cash flow and fraud risk to capital requirements, capital structure and capital efficiency. The impact of payments decisions reaches through the balance sheet to the value of the business itself.

At SunTrust, we want to help you link your business plans, your capital requirements and your payments programs to generate the success that you seek. Mr. Maza adds, "We leverage our payments expertise and our knowledge of market trends to advise clients on the right payments mix for their specific needs, ranging from traditional to electronic methods that best support their smart growth strategy."

More detailed information on successful payments strategies and techniques can be found in our in-depth reports:

Directing Payments

Managing Collections

Protecting from Fraud

Reporting and Controlling Cash

Reach out to your SunTrust Relationship Manager or Treasury Sales Officer to discuss your business plans for smart growth and your payments needs. With our SunTrust OneTeam Approach℠, SunTrust brings the resources you need to support you and your business, whether seeking capital, working on financial systems, exploring strategic options or securing you and your family's future.

To find out more, call your SunTrust Relationship Manager or visit the **SunTrust Resource Center** for more information.

About our Research

In today's world with technical and regulatory complexity, business executives need to be able to call on the right expertise to get to the most salient points without information overload. For our *Developing Strategies for the Electronification of Payments* series of reports, SunTrust has combined the results of our periodic research with over 500 Middle Market and Small Businesses with insights from an assembled team of SunTrust executives and industry leaders.

Michael Maza — Head of SunTrust Treasury & Payment Solutions

Robert Blair — Product & Digital, SunTrust Treasury & Payment Solutions

Magnus Carlsson — Manager of Treasury & Payments, Association for Financial Professionals (AFP)

Chris Fritz — Digital Solutions, SunTrust Treasury & Payment Solutions

Kellie Goodwin — Wholesale Payments Strategy, SunTrust Corporate Strategy Group

Carolyn Pyle-Kennedy, CTP — Technical Product Consulting, SunTrust Treasury & Payment Solutions

David Sawyer, CPA, CFE — Partner, Frazier & Deeter, LLC

Works Cited

The 2013 Federal Reserve Payments Study. Federal Reserve System. July, 2014.

AFP Payments Fraud and Control Survey. Association for Financial Professionals (AFP). 2016.

Report to the Nations on Occupational Fraud and Abuse Global Study. Association of Certified Fraud Examiners (ACFE). 2014. http://www.AFPonline.org/fraud.

Weise, Elizabeth. (2014, September 24). 43% of companies had a data breach in the past year. USA Today. Accessed 2/2/16.

SUNTRUST