Combatting Treasury Fraud: External forces changing the cybercrime and cyber-fraud landscape
“Cyber threats that were previously unthinkable are now daily news”\(^1\). With the threat to treasury teams continuously morphing, finance professionals need to be well prepared. We partnered with Celent to explore this topical issue and have discovered that many treasury teams are not as prepared as they need to be.

The report highlights that a full 77% of organisations have not yet identified a cyber scenario that could affect them and over one third (37%) do not have an understanding of their exposure to cyber risk. To complicate matters, the research emphasises the key risk that all treasurers must grapple with: that cybercrime and the cyber fraud landscape is constantly shifting with an ever-growing range of attack mechanisms and increasingly sophisticated tools.

Two attack vectors in particular stand out: the use of ransomware and the rise of treasury fraud. Both are explored in this report, including specifically, how business email compromise and internal fraud remain key threats to treasurers.

As custodians of an organisation’s cash, treasurers have a key role to play in the fight against cybercrime. By being strategic about this issue, treasurers can go a long way to mitigating the threat. To help you, the report highlights some of the best practices that treasurers should adopt, including taking a risk based approach, better using technology and education and the role of insurance.

I hope you find this an informative read.

---

As custodians of an organisation’s cash, treasurers have a key role to play in the fight against cybercrime.

---

\(^1\) Marsh & McLennan Cyber Handbook, 2016
This report was commissioned by HSBC Bank Plc. ("HSBC") at whose request Celent developed this research. The analysis, conclusions and opinions are Celent's alone, and HSBC had no editorial control over the report contents.
CONTENTS

INTRODUCTION.............................................................................................................. i

THE CYBERCRIME AND CYBERFRAUD LANDSCAPE ............................................... 1

FOCUS ON RANSOMWARE.................................................................................. 3

FOCUS ON TREASURY FRAUD......................................................................... 3

FIGHTING BACK: WHO IS DOING WHAT? ................................................................. 7

BEST PRACTICES ......................................................................................................... 8

TAKING A RISK-BASED APPROACH...................................................................... 8

LEVERAGING TECHNOLOGY.............................................................................. 9

MINIMISING RISK........................................................................................... 10

THE PATH FORWARD................................................................................................. 12

APPENDICES ............................................................................................................... 14

ABOUT OUR RESEARCH ............................................................................................. 17

USING SEASONED PROFESSIONALS................................................................. 17

AN UNPARALLELED NETWORK.............................................................................. 17

ROBUST RESEARCH METHODOLOGY AND INDEPENDENCE .................... 17

RELATED CELENT RESEARCH.............................................................................. 18
“The cyberthreats that many companies previously considered to be unthinkable are now daily news. To avoid becoming another headline, organizations must prepare for the worst — including the unthinkable.”

INTRODUCTION

Many treasurers are tasked with understanding and mitigating cyber-risks. That is due in part to the fact that corporate treasurers’ responsibilities have expanded significantly in recent years to include management of the company’s complex risks, regulatory oversight, and treasury technology. Treasurers also have ultimate responsibility for many of the areas most commonly targeted by cybercriminals, including cash balances, global bank connectivity, high-value payments processing, and maintenance of repetitive payment instructions.

82% of treasurers cited cybersecurity as their number one concern

The treasury and finance professionals who responded to the ACT’s annual survey cited “cybersecurity” as their number one concern (82%), followed by “other geographical uncertainty excluding Brexit” (69%), and financial markets volatility (67%). With breaches becoming more frequent and severe, it’s no surprise that treasurers are prioritising cybersecurity.

The report looks at how corporate treasury organisations can centralise, automate, and streamline management, technologies, processes, and controls for a sounder and more resilient cybersecurity and cyberfraud framework.

1Go to Cyber Extremes: What to do when Digitalization Goes Wrong, Claus Herbolzheimer, MMC Cyber Handbook 2016, Marsh & McLennan Companies’ Global Risk Center
2The Business of Treasury 2017, Association of Corporate Treasurers (ACT), 2017
THE CYBERCRIME AND CYBERFRAUD LANDSCAPE

“Even though the number of targeted cyberattacks is growing by double digits annually, many medium and large-sized corporations still do not devote sufficient resources to cyber-risk management.”

THE STATE OF CYBER RISK MANAGEMENT AT A GLANCE

- **70%** The percentage of organisations that have not developed a cyber incident response plan.
- **46%** The percentage of organisations that have not implemented or enhanced their phishing awareness training for employees in the past 12 to 24 months.
- **43%** The percentage of organisations without board-level responsibility for the review and management of cyber risk.
- **37%** The percentage of organisations that have not estimated the financial impact of a cyber attack.
- **34%** The percentage of organisations that do not assess their suppliers or customers for cyber risk.

*Source: 2017 Marsh/Microsoft Global Cyber Risk Perception Survey, Ocean analysis.*

As shown in the above graphic, based on the Marsh/Microsoft Global Cyber Risk Perception Survey, 70% of organisations have not developed a cyber incident response plan, and 43% of organisations do not have board-level responsibility for the review and management of cyber-risk.

The cybercrime and cyberfraud landscape is constantly shifting, with a wider range of attack vectors and more sophisticated attack tools. The graphic below from digital identity provider ThreatMetrix details attack vectors across five major categories. **Appendix 1** describes each of those categories.
In the Marsh/Microsoft Global Cyber Risk Perception Survey, organisations recognised a wide variety of threats arising from cyberattack vectors, with business interruption (75%) ahead of reputational loss (59%) as the number one threat deriving from loss scenarios. Recent high-profile cyberattacks, after which companies have seen their operations disrupted, have raised awareness of their capacity to impact daily business operations.
Although the list of rapidly evolving attack vectors is a long one, two stand out. One, ransomware, rose to prominence in 2017 and the other, treasury fraud, is a growing concern of finance professionals.

**FOCUS ON RANSOMWARE**

WannaCry, Petya, GoldenEye, CryptoLocker, Locky — ransomware is a constant presence in the 2017 news cycle. According to the Europol European Cybercrime Centre (EC3), ransomware is malware that locks your computer and mobile devices, or encrypts your electronic files, demanding that a ransom be paid (often using bitcoin) in order to regain control of your data.

Ransomware can be downloaded through fake application updates or by visiting compromised websites. Malicious emails disguised as routine correspondence, such as invoices or delivery notifications, were the favoured means of spreading ransomware. In 2016 security firm Symantec detected 463,841 ransomware attacks with an average ransom amount of US$1,077, up from US$294 a year earlier.

Bitcoin remains the currency of choice for the payment for criminal products and services in the digital underground economy and the Darknet. Bitcoin has also become the standard payment solution for extortion payments.

According to *The Guardian*, victims of WannaCry were asked to pay between $300 (£228) and $600 in ransom to unlock the files taken hostage by the malware. About 230,000 computers worldwide are believed to have been infected. Three months after the May 2017 attack, hackers withdrew £108,000 of bitcoin ransom, as law enforcement tried to track owners’ bitcoin accounts by following the transactions in bitcoin’s blockchain distributed ledger.

**FOCUS ON TREASURY FRAUD**

Treasury-specific threats include payment fraud, supplier fraud, business email compromise, imposter fraud, ransomware, account takeover, and fake invoices and purchase orders.

---

3Internet Security Threat Report, Volume 22, Symantec, April 2017
4WannaCry: hackers withdraw £108,000 of bitcoin ransom, Samuel Gibbs, The Guardian, 3 August 2017
PAYMENTS FRAUD

According to the Association for Financial Professionals (AFP), after a period of substantial declines, payments fraud is on the increase.

“74% of finance professionals report that their companies were victims of payments fraud in 2016. This is the largest share on record, exceeding the previous record-high share of 73% in both 2009 and 2015, and significantly higher than the percentages reported between 2011 and 2014. It suggests that fraudsters are continuing to succeed in their attempts to attack organizations’ payment systems”.

The AFP says that 36% percent of respondents whose organisations experienced payments fraud report that the fraud attempts increased in 2016 compared to 2015. Not surprisingly, larger organisations with annual revenue of at least $1 billion were more likely than smaller companies to have experienced an increase in fraud activity over the past year.

Analysing the AFP trend data, Celent calculates that the overall rise in payments fraud from 2013 to 2016 was largely driven by a 229% increase in wire fraud, the preferred payment method for Business Email Compromise (BEC) scams.

---

52017 AFP Payments Fraud and Control Survey, Association for Financial Professionals
According to the AFP, the fact that wire fraud is being reported at an elevated level indicates that BEC scams, unfortunately, continue to be prevalent and effective.

**BUSINESS EMAIL COMPROMISE**

According to the US Federal Bureau of Investigation, Business Email Compromise (BEC) and Email Account Compromise (EAC) scams continue to grow, evolve, and target small, medium, and large businesses. BEC is defined as a sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The EAC targets individuals that perform wire transfer payments. As the techniques used in BEC and EAC scams have become increasingly similar, the IC3 began tracking these scams as a single crime type in 2017.

Trend Micro’s 2017 Midyear Security Roundup indicates that US corporates should particularly be on alert. Thirty-one percent of BEC scams so far in 2017 have been against companies in the United States, followed by Australia (27%), the UK (22%), Norway (5%), and Canada (3%).
Money mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds to another bank account, usually outside the US. Upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme. IC3 also found that Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom have also been identified as prominent destinations.6

Based on complaints filed with the FBI Internet Crime Complaint Center (IC3), there are five main scenarios by which BEC and EAC fraud is perpetrated. Appendix 2 contains detailed descriptions of each of the categories.

WHICH CYBER LOSS SCENARIOS PRESENT THE GREATEST THREATS TO YOUR ORGANISATION?

1. BUSINESS WORKING WITH A FOREIGN SUPPLIER
   A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account.

2. BUSINESS EXECUTIVE RECEIVING OR INITIATING A REQUEST FOR A WIRE TRANSFER
   A request for a wire transfer from a business executive's compromised account is made to a second employee within the company who is typically responsible for processing these requests.

3. BUSINESS CONTACTS RECEIVING FRAUDULENT CORRESPONDENCE THROUGH COMPROMISED E-MAIL
   Requests for invoice payments to fraudster-controlled bank accounts are sent from a hacked employee's personal e-mail account to multiple vendors identified from this employee's contact list.

4. BUSINESS EXECUTIVE AND ATTORNEY IMPERSONATION
   Victims may be pressured by fraudsters identifying themselves as lawyers to act quickly or secretly in handling the transfer of funds; often timed to coincide with the close of business of financial institutions.

5. DATA THEFT
   Fraudulent requests for W-2 or personally identifiable information (PII) data, using a business executive's compromised e-mail, are used to impersonate targeted employees.

---

6US Federal Bureau of Investigation Public Service Announcement, Alert Number I-050417-PSA, May 4, 2017

INTERNAL/OCCUPATIONAL FRAUD

According to the Association of Certified Fraud Examiners (ACFE), internal fraud, also called occupational fraud, occurs when an employee, manager, or executive commits fraud against their employer.

In the ACFE’s most recent global study of its occupational fraud cases, the total loss exceeded US$6.3 billion, with an average loss per case of $2.7 million. The highest percentage of fraud cases involved asset misappropriation (83%), including false billing schemes, pilfering inventory, stealing payments in transit, and altering cheques. Descriptions of each of the categories can be found in Appendix 3.

---

6US Federal Bureau of Investigation Public Service Announcement, Alert Number I-050417-PSA, May 4, 2017
The ACFE also surveyed respondents about the steps fraudsters took to conceal their schemes. Creating and altering physical documents were the most common fraud methods, but fraudsters also manipulated accounting system transactions, altered electronic documents, and deleted journal entries.

**FIGHTING BACK: WHO IS DOING WHAT?**

The fight against cybercrime is entering a new era of collaboration. A few examples include:

- In late 2016, officials from agencies in 30 countries — including the US Justice Department, Europol, and the United Kingdom’s National Crime Agency — collaborated with private cybersecurity companies and academics to take down an extensive online criminal infrastructure called “Avalanche.” Criminals had been using the platform since 2009 to mount phishing attacks, distribute malware, shuffle stolen money across borders, and even act as a botnet in denial of service attacks.7

- In early 2016, law enforcement agencies and judicial bodies from Belgium, Denmark, Greece, the Netherlands, the United Kingdom, Romania, Spain, and Portugal — with further support from Moldova and other countries — joined forces in the first coordinated European action against money muling. The operation was also supported by Europol, Eurojust, and the European Banking Federation (EBF).8

- The United Kingdom is opting into a new intelligence-sharing program with EU law enforcement agency Europol, in an effort to boost cross-border action against terrorism and cybercrime.9

---

7It Took 4 Years to Take Down “Avalanche,” a Huge Online Crime Ring; Lily Hay Newman, Wired, 02 December 2016
8Europe-wide Action Targets Money Mule Schemes, Europol press release, 01 March 2016
9UK opts in to new Europol intelligence-sharing programme, Helen Warrell, Financial Times, 14 November 2016
• The Financial Services Information Sharing and Analysis Center (FS-ISAC) is extending its US charter to share information between financial services firms worldwide.10

There are six key interconnected and interrelated groups joining forces in various combinations to combat cybercrime and cyberfraud:

INTERCONNECTED AND INTERRELATED GROUPS JOINING FORCES

1. REGULATORS
   Strengthening regulatory framework e.g. EU Network and Information Security Directive, US Cybersecurity Act, EU General Data Protection Regulation (GDPR), ASEAN Cyber Capacity Program (ACCP).

2. LAW ENFORCEMENT
   Increasing public/private collaboration between public agencies and with private security professionals e.g. No More Ransom!, European Money Mule Action, Shadowserver Foundation, and INTERPOL Global Complex for Innovation.

3. FINANCIAL INSTITUTIONS
   Comprehensive cybersecurity framework, periodic risk assessments, continuous monitoring, extensive controls, internal and customer education, and fraud prevention services including complimentary antivirus software, white list services, IP filtering, strong authentication, and payment change alerts.

4. FINANCIAL NETWORKS

5. INDUSTRY GROUPS
   ECB Committee on Payments and Market Infrastructures (CPMI)/Board of the International Organization of Securities Commissions (IOSCO) guidance on cyber resilience, AICPA System and Organization Controls for Cybersecurity.

6. TECHNOLOGY PROVIDERS
   Incorporating emerging technologies such as behavioural analytics, artificial intelligence, risk scoring, behaviour-based profiling.

Source: Celent

BEST PRACTICES

Celent believes that cybercrime and cyberfraud must be recognised as technology, operational, and business issues, not just an IT departmental mandate. Cybersecurity must be managed holistically and closely aligned to a firm’s enterprise risk and operational risk frameworks.

TAKING A RISK-BASED APPROACH

As discussed in Treating Cyber-Risk as an Operational Risk (October 2016), a starting point for many organisations (including financial institutions) is to use the National Institute of Standards and Technology (NIST) framework as the foundation for more mature and sustainable cybersecurity management. The purpose of the framework is to elevate cyber-risk at the corporate level and to enable institutions:

“Regardless of size, degree of cybersecurity risk, or cybersecurity sophistication — to apply the principles and best practices of risk management to improving the security and resilience of critical infrastructure.”11

The framework provides a structure and means to manage cybersecurity by assembling standards, guidelines, and practices that are working effectively in industry today. The NIST framework is organised along five interconnected functions that are known across the industry as the Cyber Kill Chain: Identify, Protect, Detect, Respond, and Recover.

LEVERAGING TECHNOLOGY

Enterprises can leverage technology to sustain a risk-based approach to cyber-risk management. This requires technologies that enable organisations to monitor complex and large volumes of data and run advanced data crunching analytics to identify potential vulnerabilities, incidents, and their impact. Very few firms should be going this alone; organisations need dedicated expert partners and advanced technical capabilities. *Treating Cyber-Risk* provides a sampling of cybersecurity technology vendors and consulting firms with solutions aligned to the NIST security framework, and highlights the importance of a layered approach to identifying, protecting, detecting, responding, and recovering to cyberthreats.
The layered approach is reflected in controls mandated by banking regulators. For example, since 2012 the FFIEC has required US financial institutions to implement a layered security program for high-risk Internet-based systems that include fraud detection and monitoring systems, multifactor authentication, enhanced controls over account activities, enhanced control over account maintenance activities, and enhanced customer education.\(^{12}\)

Selection of the right security vendor, partner, and/or product is challenging not only because of the complexity of the vendor landscape, but also because the institution is not always certain of what it needs to protect. Siloed purchases, defensive purchases, or bowing to executive pressure to purchase the latest and greatest security tool have proven to be ineffective. The best way to avoid shelfware is to better educate the decision-makers on how breaches happen, why they are not addressed earlier, and what steps need to be taken to prevent a breach. The focus should then become selecting the right expertise, identifying the issue, and then purchasing the right product.

**MINIMISING RISK**

At a tactical level, organisations can implement relatively straightforward policies to minimise ransomware and treasury fraud, two of the most prevalent risks facing organisations.

**RANSOMWARE**

To prevent ransomware from being downloaded through fake application updates, visiting compromised websites, email attachments, or other malware, Europol’s European Cybercrime Centre advises the following measures:

---

\(^{12}\)FFIEC Supplement to Authentication in an Internet Banking Environment, Financial Institution Letter FIL-50-2011, June 29, 2011
Chapter: Best Practices

TREASURY FRAUD

In its 2017 survey, AFP identified a variety of actions that corporates are taking to defend against attacks. The most frequent action taken is to perform daily reconciliations (74%). Other actions include restricting payments access to company-issued laptops, and not using mobile devices except for emergency situations.

EDUCATION

Corporate treasurers can learn more about preventing cybercrime and cyberfraud from a number of sources including Interpol, Europol, FBI, National Security Agency (NSA), National Institute of...
Standards and Technology (NIST), and their banking partners. Many banks maintain educational microsites, publish white papers, host webinars, or organise seminars on cybersecurity strategies and tactics.

**CYBERSECURITY INSURANCE**

As proactive cyber-risk management increases, the purchase of cyber risk insurance is also increasing. The MMC Cyber Handbook 2016 states that total annual cyber premiums have reached an estimated $2 billion and may reach $20 billion by 2025. The US remains the largest cyber insurance market; nearly 20% of all organizations have cyber insurance, and there are yearly increases in the number of companies purchasing cyber insurance, and increases in the limits. Interest in cyber insurance is growing in other markets. For example, a recent Marsh survey of European Risk Managers found that nearly 25% planned to explore cyber insurance options over the next 24 months, and a survey of UK risk managers shows that 20% of companies are buying insurance.

**THE PATH FORWARD**

“Boards and executive management need to look critically at the level of preparedness of their organization for the increasing risk of cyberattacks and invest to close gaps.”

Cyber-risks are growing in terms of both their sophistication and the frequency of attacks. Fighting cybercrime and cyberfraud requires firms to address new and complex cyber-risk management challenges that will require specialized skills, but the basis of solid protection and robust management starts with leadership from the board and the recognition that cybersecurity is the responsibility of all staff. To set the cyber-risk posture of the organization, the board and management must determine the balance of how much cyber-risk to accept, how much to spend mitigating the risk, and where to accept and mitigate it.

---

13Alex Wittenberg, *The Evolving Cyber Risk Landscape*, MMC Cyber Handbook 2016, Marsh & McLennan Companies’ Global Risk Center

Overall governance must be sufficiently agile to manage for emerging threat factors, changing user behaviours, and new business opportunities. Institutions should seek to achieve a layered and risk-based approach to cybersecurity: one which goes beyond the technology aspects of cyberdefence and recognises that cyber-risk is an enterprisewide concern. An organisation’s security strategy will be continually informed by behavioural analysis of risk data and the willingness to evaluate and introduce new cyber-risk management strategies and tactics.

Was this report useful to you? Please send any comments, questions, or suggestions for upcoming research topics to info@celent.com.
APPENDICES

APPENDIX 1: ATTACK VECTOR GLOSSARY

DEVICE SPOOFING
Device spoofing techniques are widely used by fraudsters to evade device recognition and detection capabilities. Device spoofing allows a fraudster to masquerade as a legitimate customer, manipulate login sessions, open fraudulent accounts, intercept user credentials, or take advantage of multiple new account bonuses.

LOCATION MANIPULATION
Fraudsters manipulate their location tracking in order to mask their true whereabouts. Sometimes this allows them to pretend to be a legitimate customer, or to trade from a location that is perhaps blocked by a company’s business rules or banned under regulatory compliance such as OFAC.

IDENTITY FRAUD
Fraudsters are creating complete identities using a patchwork quilt of stolen identity data, harvested from data breaches and the dark web. These stolen and spoofed identities are often a near-perfect match for the “real” identity, and are used to open fraudulent new accounts, takeover existing accounts, and monetize stolen credit cards.

THREATS/BOTS
Fraudsters have a gamut of threat vectors at their disposal to perpetrate fraud, including malware, remote access Trojans (RATs), Man-in-the-Middle attacks, and automated bot attacks. These are often used in combination to perform mass identity testing attacks (via an advanced bot), and then take over a trusted user account via a Man-in-the-Middle attack and/or RAT.

BUSINESS FRAUD RISK
Risks extend beyond just fraudulent account registrations, account takeovers, and payments fraud to encompass bonus abuse, fake reviews, and OFAC breaches. The damaging effects of fraud can therefore permeate deeper than initial monetary loss, into the realms of damage to customer trust, poor Net Promoter scores, and loss of reputation, as well as regulatory breaches and subsequent fines.

APPENDIX 2: BUSINESS EMAIL COMPROMISE (BEC) AND EMAIL ACCOUNT COMPROMISE (EAC) SCENARIOS

BUSINESS WORKING WITH A FOREIGN SUPPLIER
A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent account. The request may be made via telephone, facsimile, or email. If an email is received, the subject will spoof the email request so it appears similar to a legitimate request. Likewise, requests made via facsimile or telephone call will closely mimic a legitimate request. This particular scenario has also been referred to as the “Bogus Invoice Scheme,” “Supplier Swindle,” and “Invoice Modification Scheme.”

BUSINESS EXECUTIVE RECEIVING OR INITIATING A REQUEST FOR A WIRE TRANSFER
The email accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is made to a second employee within the company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the financial institution with instructions to urgently send funds to bank “X” for reason “Y.” This particular scenario has

---

16 US Federal Bureau of Investigation Public Service Announcement, Alert Number I-050417-PSA, May 4, 2017
been referred to as “CEO Fraud,” “Business Executive Scam,” “Masquerading,” and “Financial Industry Wire Frauds.”

BUSINESS CONTACTS RECEIVING FRAUDULENT CORRESPONDENCE THROUGH COMPROMISED E-MAIL
An employee of a business has his or her personal email hacked. This personal email may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from this employee’s personal email to multiple vendors identified from this employee’s contact list. The business may not become aware of the fraudulent requests until that business is contacted by a vendor to follow up on the status of an invoice payment.

BUSINESS EXECUTIVE AND ATTORNEY IMPERSONATION
Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or email. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

DATA THEFT
Fraudulent requests are sent utilizing a business executive’s compromised e-mail. The entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipients of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated, and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario even if they were able to successfully identify and avoid the traditional BEC scam. This data theft scenario of the BEC scam first appeared just prior to the 2016 tax season.

APPENDIX 3 ASSET MISAPPROPRIATION SCHEMES

BILLING SCHEME
A fraudulent disbursement scheme in which a person causes his or her employer to issue a payment by submitting invoices for fictitious goods or services, inflated invoices, or invoices for personal purchases (e.g., employee creates a shell company and bills employer for services not actually rendered; employee purchases personal items and submits an invoice to employer for payment).

CASH LARCENY
A scheme in which an incoming payment is stolen from an organization after it has been recorded on the organization’s books and records (e.g., employee steals cash and cheques from daily receipts before they can be deposited in the bank).

CASH-ON-HAND
A scheme in which the perpetrator misappropriates cash kept on hand at the victim organization’s premises (e.g., employee steals cash from a company vault).

CHEQUE TAMPERING
A fraudulent disbursement scheme in which a person steals his or her employer’s funds by intercepting, forging, or altering a cheque or electronic payment drawn on one of the organization’s bank accounts (e.g., employee steals blank company cheques and makes them out to himself or an accomplice; employee steals an outgoing cheque to a vendor and deposits it into his or her own bank account).

EXPENSE REIMBURSEMENTS

---

17Report to the Nations on Occupational Fraud and Abuse, 2016 Global Fraud Study, ACFE
A fraudulent disbursement scheme in which an employee makes a claim for reimbursement of fictitious or inflated business expenses (e.g., employee files fraudulent expense report, claiming personal travel, nonexistent meals).

NON-CASH
Any scheme in which an employee steals or misuses non-cash assets of the victim organization (e.g., employee steals inventory from a warehouse or storeroom; employee steals or misuses confidential customer financial information).

PAYROLL SCHEME
A fraudulent disbursement scheme in which an employee causes his or her employer to issue a payment by making false claims for compensation (e.g., employee claims overtime for hours not worked; employee adds ghost employees to the payroll).

REGISTER DISBURSEMENTS
A fraudulent disbursement scheme in which an employee makes false entries on a cash register to conceal the fraudulent removal of cash (e.g., employee fraudulently voids a sale on his or her cash register and steals the cash).

SKIMMING
A scheme in which an incoming payment is stolen from an organization before it is recorded on the organization’s books and records (e.g., employee accepts payment from a customer but does not record the sale and instead pockets the money).
ABOUT OUR RESEARCH

Celent is a research and advisory firm which focusses on delivering technology-related insight to the Financial Services industry, to enable our clients to make the right decisions, at the right time.

To deliver these insights, Celent harnesses three core principles.

USING SEASONED PROFESSIONALS

Our analysts come from a wide range of backgrounds, but they all bring wide ranges of experience with them. Often the source of an insight that an analyst brings is from their previous life of having dealt with an identical situation. Celent analysts have often walked in the shoes of their clients, rather than studied it in an academic way at arm’s length, and so they understand what matters, and the nuances of the situation.

AN UNPARALLELED NETWORK

Celent’s research clients include financial institutions, vendors, and consulting firms, from around the world. In addition, we interact with the broader community, from industry bodies to regulators to journalists. Every day brings new questions, giving Celent a unique insight into the pulse of the industry, and how each party in the co-system perceives often the same issue. Equally, this network is a powerful tool for Celent to tap into as it seeks answers or validation to questions.

ROBUST RESEARCH METHODOLOGY AND INDEPENDENCE

Celent uses a variety of methodologies in its reports. For this type of report, we start with posing three key research questions. Based on our interactions with our clients, these are the questions that our clients are seeking answers to, or, using our experience and insights from previous questions, the questions that they now ought to be considering.

The research is carried to address these questions, through primary and secondary methods. We are careful to separate fact and opinion, and will always seek to validate or corroborate those facts. Information furnished by others, upon which all or portions of this report are based, is believed to be reliable but has not been independently verified, unless otherwise expressly indicated. Public information and industry and statistical data are from sources we deem to be reliable; however, we make no representation as to the accuracy or completeness of such information.

As a consequence, the findings contained in this report may contain predictions based on current data and historical trends. Any such predictions are subject to inherent risks and uncertainties.
RELATED CELENT RESEARCH

FINANCIAL CRIME MITIGATION IN THE NEW NEW WORLD OF BLOCKCHAIN
October 2017

FUTURE PROOFING PRIVACY: GDPR COMPLIANCE IN A NETWORKED BANKING SYSTEM
OLIVER WYMAN
June 2017

INDUSIND BANK: GROWING REVENUE WHILE MANAGING FRAUD
April 2017

BANKER’S GUIDE TO THIRD PARTY RISK MANAGEMENT: STRATEGIC, COMPLEX, AND LIABLE
December 2016

TREATING CYBER-RISK AS AN OPERATIONAL RISK: GOVERNANCE, FRAMEWORK, PROCESSES, AND TECHNOLOGIES
October 2016

RISK OUTLOOK FOR BANKING: CALMER TIMES
June 2016

MARKET SURVEILLANCE TRENDS: TECHNOLOGY AND EUROPEAN REGULATION TAKE CENTER STAGE
May 2016

BANKING IN THE CLOUD: BETWEEN ROGUES AND REGULATORS, PART 2
April 2016

CELENT MODEL BANK 2016, PART VI: CASE STUDIES IN SECURITY, FRAUD, AND RISK MANAGEMENT
March 2016

STRESS TESTING SOLUTIONS 2016, PART 1: FUTURE ARCHITECTURAL BEST OR ARCHITECTURAL MESS?
March 2016

NEXT-GENERATION RISK APPETITE MANAGEMENT: GETTING REAL ABOUT ACHIEVING IMPACT IN UNCERTAIN TIMES
March 2016

REGTECH RISING: COMPLIANCE AS A SERVICE PUZZLE
February 2016

GOVERNING RISK: A TOP-DOWN APPROACH TO ACHIEVING INTEGRATED RISK MANAGEMENT
January 2016
For more information please contact info@celent.com or:

Patricia Hines  phines@celent.com
Gareth Lodge  glodge@celent.com
Alenka Grealish  agrealish@celent.com

<table>
<thead>
<tr>
<th>AMERICAS</th>
<th>EUROPE</th>
<th>ASIA</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>200 Clarendon Street, 12th Floor</td>
<td>28, avenue Victor Hugo</td>
<td>The Imperial Hotel Tower, 13th Floor</td>
</tr>
<tr>
<td>Boston, MA 02116</td>
<td>Paris Cedex 16</td>
<td>1-1-1 Uchisaiwai-cho</td>
</tr>
<tr>
<td>Tel.: +1.617.262.3120</td>
<td>Tel.: +33.1.73.04.46.20</td>
<td>Chiyoda-ku, Tokyo 100-0011</td>
</tr>
<tr>
<td>Fax: +1.617.262.3121</td>
<td>Fax: +33.1.45.02.30.01</td>
<td>Tel: +81.3.3500.3023</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fax: +81.3.3500.3059</td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1166 Avenue of the Americas</td>
<td>55 Baker Street</td>
<td>Beijing Kerry Centre</td>
</tr>
<tr>
<td>New York, NY 10036</td>
<td>London W1U 8EW</td>
<td>South Tower, 15th Floor</td>
</tr>
<tr>
<td>Tel.: +1.212.541.8100</td>
<td>Tel.: +44.20.7333.8333</td>
<td>1 Guanghua Road</td>
</tr>
<tr>
<td>Fax: +1.212.541.8957</td>
<td>Fax: +44.20.7333.8334</td>
<td>Chaoyang, Beijing 100022</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tel: +86.10.8520.0350</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fax: +86.10.8520.0349</td>
</tr>
<tr>
<td>USA</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Four Embarcadero Center, Suite 1100</td>
<td>Galleria San Babila 4B</td>
<td>Singapore</td>
</tr>
<tr>
<td>San Francisco, CA 94111</td>
<td>Milan 20122</td>
<td>8 Marina View #09-07</td>
</tr>
<tr>
<td>Tel.: +1.415.743.7900</td>
<td>Tel.: +39.02.305.771</td>
<td>Asia Square Tower 1</td>
</tr>
<tr>
<td>Fax: +1.415.743.7950</td>
<td>Fax: +39.02.303.040.44</td>
<td>Singapore 018960</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Tel.: +65.9168.3998</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fax: +65.6327.5406</td>
</tr>
<tr>
<td>Brazil</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Av. Doutor Chucri Zaidan, 920 – 4º andar</td>
<td>Paseo de la Castellana 216</td>
<td>South Korea</td>
</tr>
<tr>
<td>Market Place Tower I</td>
<td>Pl. 13</td>
<td>Youngpoong Building, 22nd Floor</td>
</tr>
<tr>
<td>São Paulo SP 04578-903</td>
<td>Madrid 28046</td>
<td>33 Seorin-dong, Jongno-gu</td>
</tr>
<tr>
<td>Tel.: +55.11.5501.1100</td>
<td>Tel.: +34.91.531.79.00</td>
<td>Seoul 110-752</td>
</tr>
<tr>
<td>Fax: +55.11.5501.1110</td>
<td>Fax: +34.91.531.79.09</td>
<td>Tel.: +82.10.3019.1417</td>
</tr>
<tr>
<td>Canada</td>
<td></td>
<td></td>
</tr>
<tr>
<td>1981 McGill College Avenue</td>
<td>Tessinerplatz 5</td>
<td>Fax: +82.2.399.5534</td>
</tr>
<tr>
<td>Montréal, Québec H3A 3T5</td>
<td>Zurich 8027</td>
<td></td>
</tr>
<tr>
<td>Tel.: +1.514.499.0461</td>
<td>Tel.: +41.44.5533.333</td>
<td></td>
</tr>
</tbody>
</table>