AFP 2020 VIRTUAL EXPERIENCE 10/19-10/29

Fraud Protection:

Treasury & IT Collaborate

GM

xylem Let's Solve Water

Today's Participants ...

Patricia Lau
Treasury Manager – Global Funding,
General Motors

Aaron Johnston
Treasury Manager, Xylem

Kiyoshi Garduno
Treasury Business Sustain Manager,
General Motors

Wade Bicknell
Chief Security Officer, Americas,
Deutsche Bank

Today's Objectives ...

Protecting our treasury operations against fraud in collaboration with IT

1 Identifying the attack ...

- Business email compromise awareness
- Outlook into emerging threats

2 Implementing best practices

- What should Treasurers and Payment Specialists be doing?
- How have past circumstances shaped present and future initiatives and campaigns?

3 Leveraging IT to drive security

- Proactively develop partnerships with IT
- Work with industry experts to deploy technology combating human error

1

Cyber Attack Process Breakdown

BUSINESS EMAIL COMPROMISE

Step 1

Criminal identifies organization's weaknesses through open source intelligence, social engineering, and scanning for vulnerabilities

Step 2

Criminal develops malware specifically for organization by exploiting identified weaknesses

Step 3

Criminal delivers malware to target through multiple channels, e.g., email attachments, compromised websites, and USB devices

Step 4

Criminal establishes direct and persistent access, spreads and activates malicious code, collects operational details, and attempts lateral movement

Step 5

Criminal identifies and steals data of value to attacker

Step 6

Criminal withdraws, removing tracks

AFP 2020

2

Industry Best Practices

Treasury & Payment Specialists principles to combatting cyber attacks

Improve your payment process…

- Understand your payment platforms
- Identify payment initiators who can also stop and/or alter payments
- Clear-cut process to reconcile routing and account information

… Implement technology controls …

- Constantly alter and use complex passwords
- Rebuild or exchange hardware on a regular basis
- Filter your email, ensuring all external mail goes to an external folder
- Adopt email intercept-based protocol
- Understand your organization's liability/policy against cyber fraud and data

… Staff training and raising awareness is imperative

- Initiate targeted campaigns to identify vulnerabilities
- Share best practices; develop forums to keep the dialogue constant
- Don't be afraid to speak up on fraud; be a voice in preventing cyber fraud in the organization
- Develop a proactive and coherent partnership with your CISO organization

3

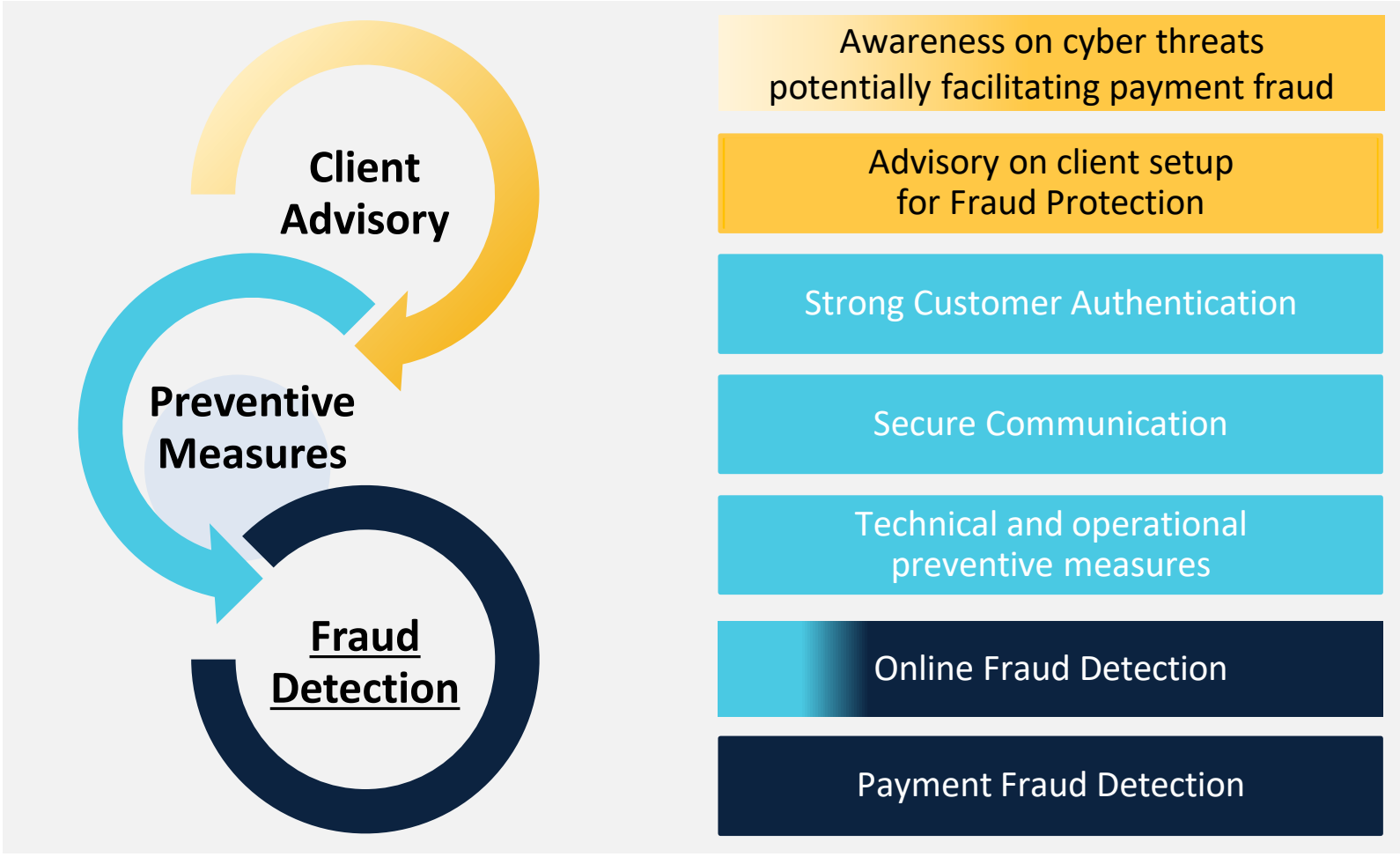
Protect Corporates from fraudulent payments by jointly delivering Awareness and Advisory as well as services for Fraud Prevention and Detection

Identify potentially fraudulent transactions in real time, across channels, payment types and regions, based on latest technologies like machine learning and artificial intelligence

Embed within your digital client experience, empowering Corporates through automation, self-service and transparency

AFP 2020

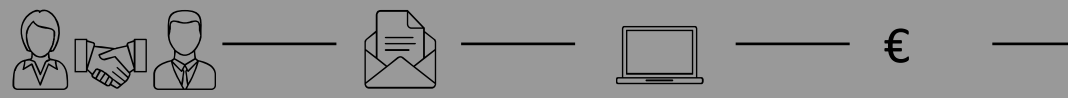
A systematic framework for payment fraud protection



3 Ways in which we can support Corporates and stakeholders alike in the future

Consistently upgrade / fine-tune rules and fraud detection models to better detect real instances of fraud. Using rules, such as identifying first time payees, may be very useful to stop such deception techniques as Invoice Redirect Fraud.

Example 'Attack' Method: Invoice Redirect Fraud



Client Relation → Manipulation request → Human mistake → Fraudulent Payment

Surveillance Engine

DB Fraud Detection	Client Action	Txn stopped / investigated
Scan payment transaction, identify a first-time payee, and inform party via notification or hold payment	Party reviews the transaction and concludes payment should not be made to new account. Party action may be to stop the payment or a funds recover request	Anti Fraud measures have been successful in the fight against fraud, and no funds lost.

AFP 2020

3

Building a digital, automated, client-empowered Experience

Provide corporates and stakeholders a superior client experience founded in the principles of digitalization, autonomy and self-service. Build an automated solution where corporates and stakeholders can receive and act on surveillance alerts with minimal reliance on bank partner, unless required. Enable fraud specific entitlements to ensure greater protection against fraud including client-defined rules and analytics

Rule Setting	• Self-service engine to set individual rules via online platform • Parameters for black / white lists may include: *Threshold, Beneficiary Country, Currency, Payment Product, Payment frequency*
Alert Handling	• Real-time alerts based on individual profiles • Assistance from fraud service team if required
KPI Provision	• Statistics and trends • Audit trail of payment alert handling

AFP 2020

Key Takeaways …

Protecting our treasury operations against fraud in collaboration with IT

- Business email compromise is a consistent and evolving attack that will never go away – build protocol to identify these emerging threats
- In partnership between Treasury, IT, and industry-wide forum, develop and share best practices – everyone wins when the bad guys lose
- Deploy technology to combat fraud – human error continues to be a leading vulnerability

CONTACTS

Patricia Lau
patricia.k.lau@gm.com

Kiyoshi Garduno
kiyoshi.garduno@cadilac.com

Aaron Johnston
aaron.Johnston@xyleminc.com

Wade Bicknell
wade.bicknell@db.com