Payment related risks – Update
Unstructured Payments

Valentin Suter

INTERNAL

CREDIT SUISSE

Payment related risks

Integrity of payment instructions and authorization pose high risk exposure

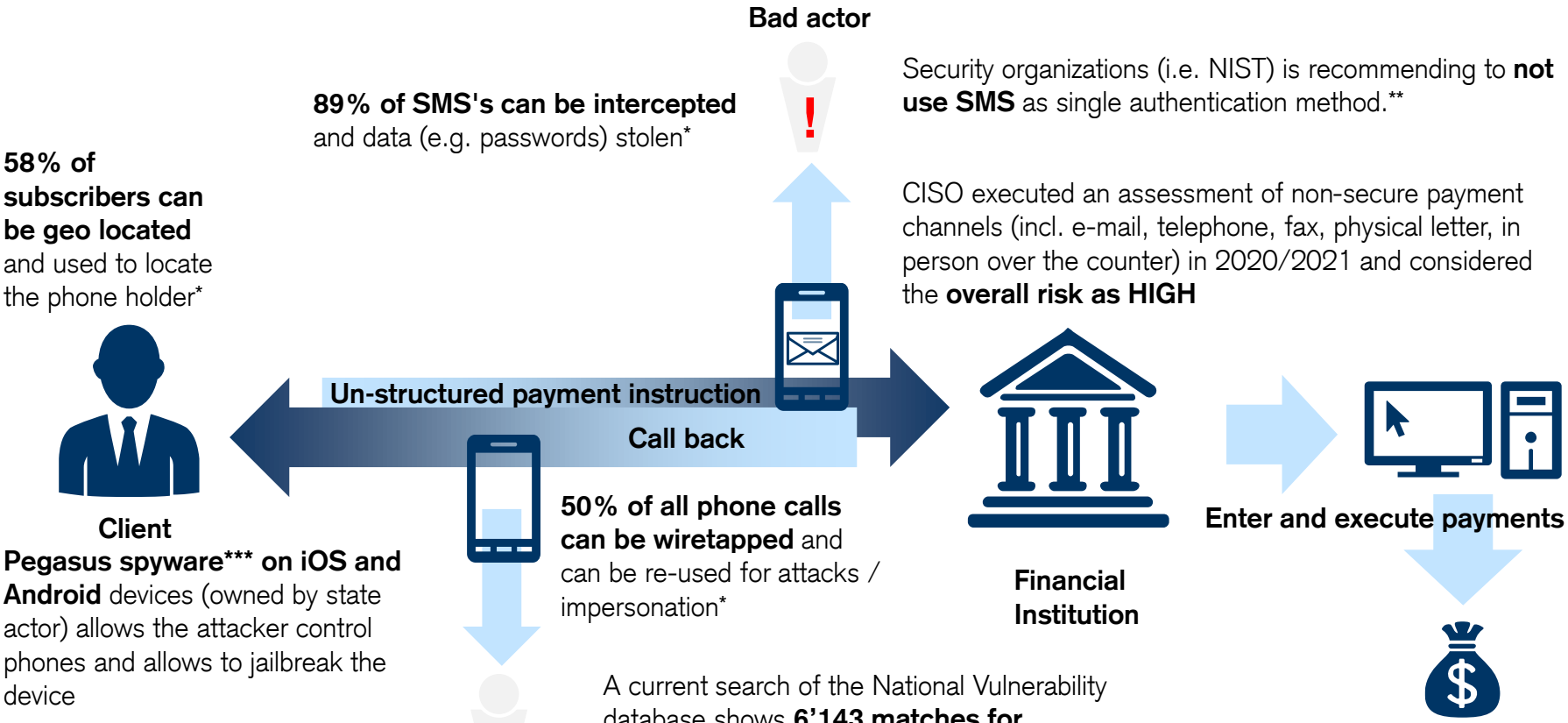
- In November 2020, CISO did complete the assessment of the payment systems in IWM locations to evaluate the risk of missing integrity controls.
- As a follow-up, CISO together with IWM Operations did investigate the technology risks around execution of call backs to authorize payments.

- The bank is facing direct loss due to incidents related to call backs and risks in security controls to ensure integrity.
- The technological threat on used technology is increasing:
  - **50% of all phone calls can be wiretapped** and can be re-used for attacks / impersonation. **89% of SMS can be intercepted. 86% us vulnerable Android OS with full rootkits available** (e.g. able to divert inbound calls from CS numbers).
  - Threat of **e-mail compromise and phishing mails is increasing** and leading to fraudulent payments.
  - **Deep fake can be used to impersonate** the clients or malware used by attackers to take over the devices or forward calls.
  - More than ever since COVID, business is done on cell phones rather than desk phones.
- Technology and business related risks are valid for all un-structured payments protected by call backs, which puts a transaction **volume higher than x bnCHF for IWM and SUB at risk**. **APAC and IB numbers are not known, but they are also exposed to the risk**.

- Based on recent incidents related to calls backs or e-mail compromise and considering the fast changing threat landscape of payments, the risk of un-structured payments is increasing and therefore mitigation measures should be evaluated.

Call back technology threat landscape

Examples of technology focused attack scenarios



Source:
* = Research on the security systems of the world's largest mobile operators conducted by Positive Technologies
** = Article on AET Europe (link) and NIST Guideline (link) / *** = Spyware sold to governments (link)

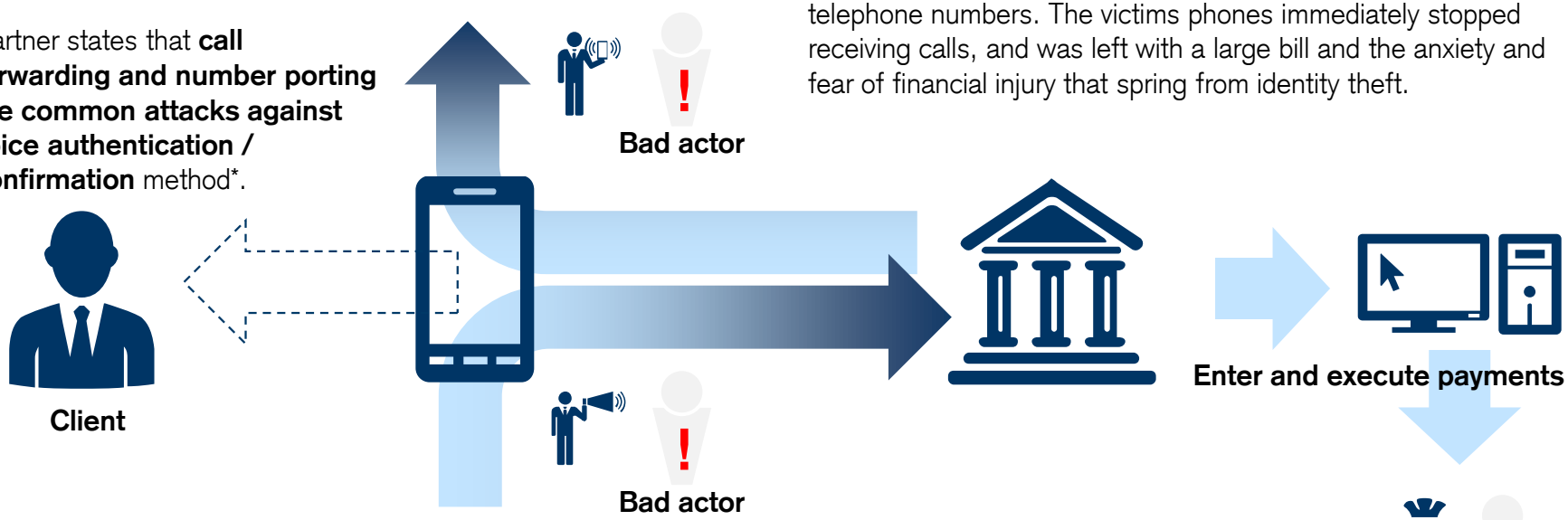
Call back technology threat landscape

3 related external incidents – SIM swap and impersonation

A Hacker Got All My Texts for $16****
the hacker used a service by a company called Sakari, which helps businesses do SMS marketing and mass messaging, to reroute my messages to him.

Your mobile phone account could be hijacked by an identity thief***
An unknown person walked into a mobile phone store, claimed to be the victim, asked to upgrade victim's mobile phones, and walked out with two brand new iPhones assigned to the victims telephone numbers. The victims phones immediately stopped receiving calls, and was left with a large bill and the anxiety and fear of financial injury that spring from identity theft.

Gartner states that **call forwarding and number porting are common attacks against voice authentication / confirmation** method*.

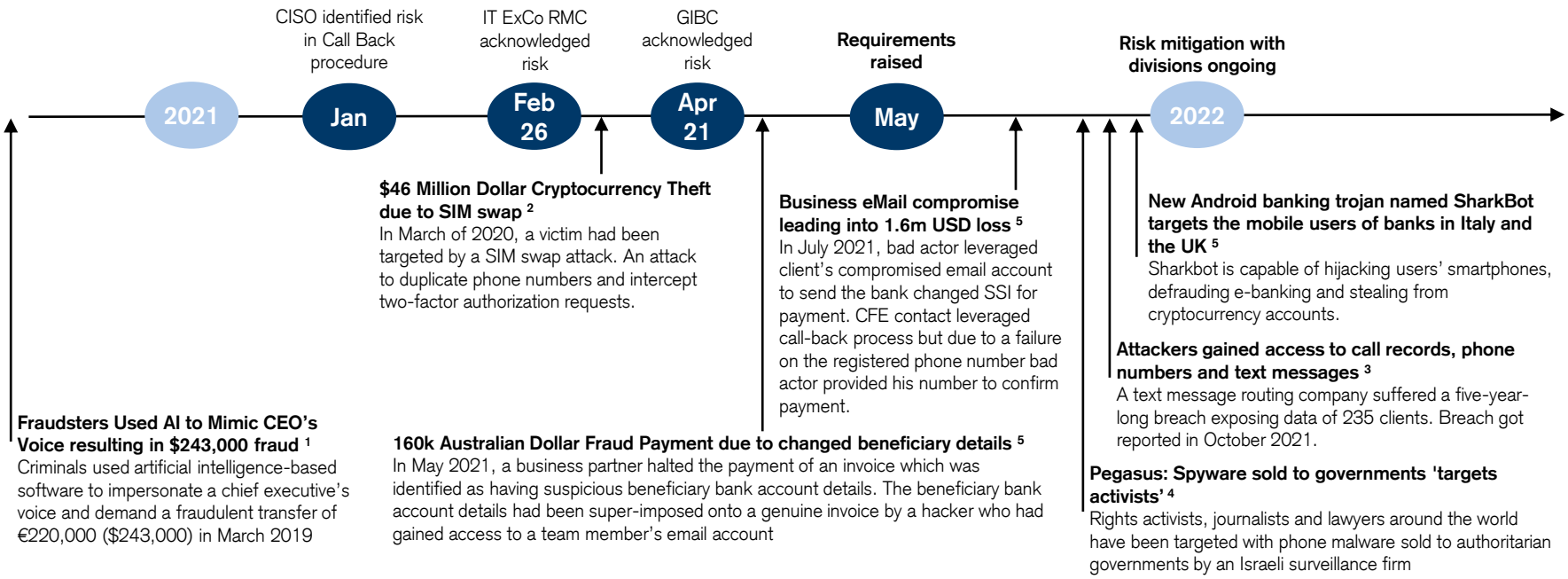


Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case**
Criminals used artificial intelligence-based software to impersonate a chief executive's voice and demand a fraudulent transfer of €220,000 ($243,000) in March 2019 in what cybercrime experts described as an unusual case of artificial intelligence being used in hacking.

Source:
* = "Decision Point for User Authentication" 28 March 2017 – Gartner
** = Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case – WSJ / Fraudsters deepfake CEO's voice to trick manager into transferring $243,000 (thenextweb.com)
*** = Your mobile phone account could be hijacked by an identity thief
**** = $16 attack shows how easy carriers make it to intercept text messages | Ars Technica

What we did and what happened related to call back

Identify risk on call back procedure and un-structured payments

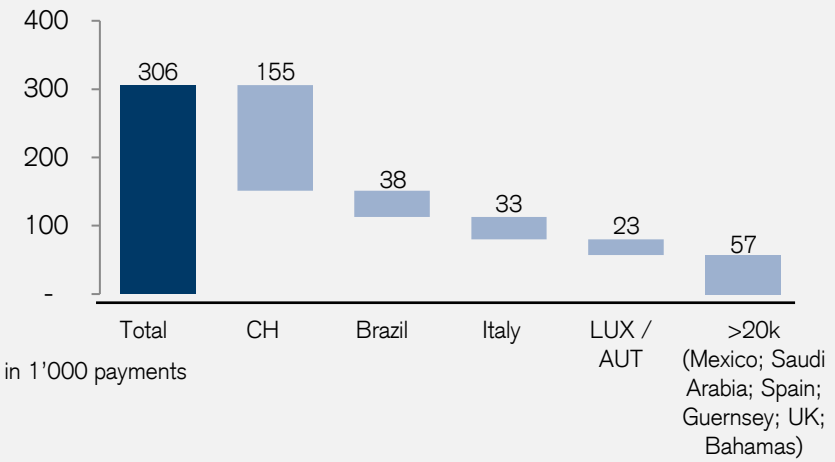


Source:
[1] = Fraudsters deepfake CEO's voice to trick manager into transferring $243,000 (thenextweb.com)
[2] = Arrest Made in $46 Million Dollar Cryptocurrency Theft (hamiltonpolice.on.ca)
[3] = A text message routing company suffered a five-year-long breach - The Verge
[4] = Pegasus: Spyware sold to governments 'targets activists' - BBC News
[5] = CS sources

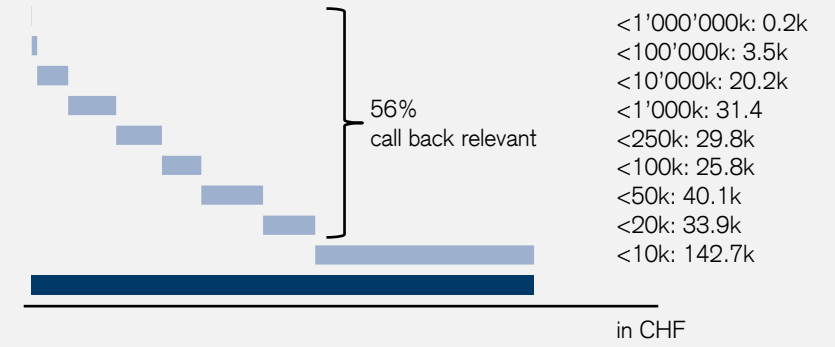
IWM Payments volume and risk exposure

Un-structured IWM Payments potentially facing call back risks

Number of un-structured payments in 2020*



Frequency of unstructured payments 2020**

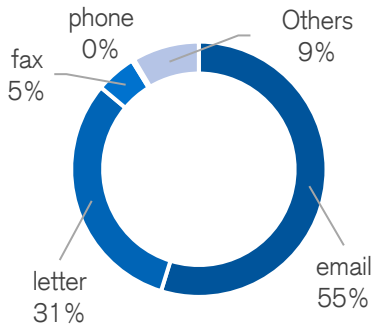


Risk exposure for **IWM**:

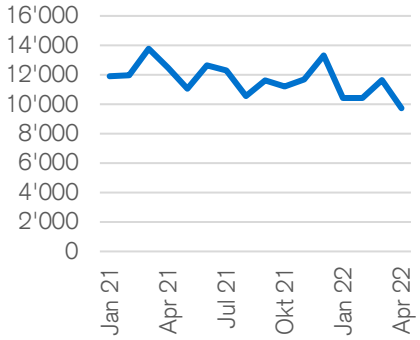
- x

Technology and business related risks are valid for all un-structured payments protected by call backs, which puts the annual **transaction volume higher than x mCHF at risk**.

Channel used to submit un-structured payments



Number of un-structured payments

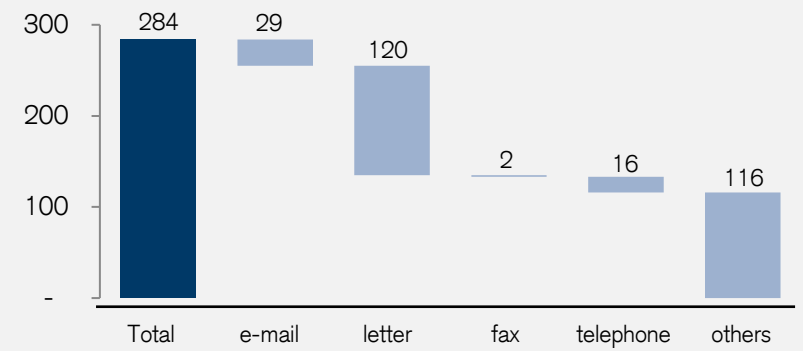


Source:
* = IWM Payments Strategy – October 2020
** = IWM Unstructured Payments 2020, Amount Classes in CHF – only IWM payments on SBIP

SUB Payments volume and risk exposure

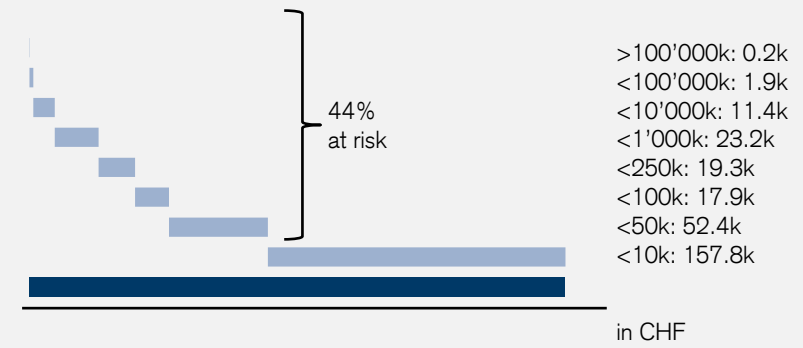
Un-structured SUB Payments potentially facing call back risks

Channel of un-structure payments 2020 in SUB (PoFo)*



in 1'000 payments

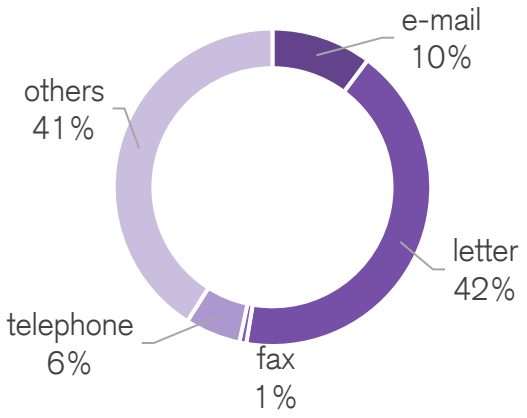
Frequency of unstructured payments 2020 in SUB (PoFo)*



Source:
* = BSP CII Weekly POFO Working Group

Technology and business related risks are valid for all un-structured payments protected by call backs, which puts the annual **transaction volume higher than x mCHF based on xk un-structured payment instructions at risk**.

Out of the un-structured payments, **10% got submitted by mail, 1% by fax, 6% during a telephone call and 42% on physical letter**. Others is referring to internal instructions, therefore exposed to insider threat.



Way forward of risks on call back

Investigating alternatives to strengthen call back procedure?

Industry statement:

- Gartner has deprecated the use of static knowledge based authentication (KBA). Organizations should look for alternatives to KBA but if they must use it, they should apply multiple protection layers and introduce additional security controls that do not rely on secret data.*

CISO view:

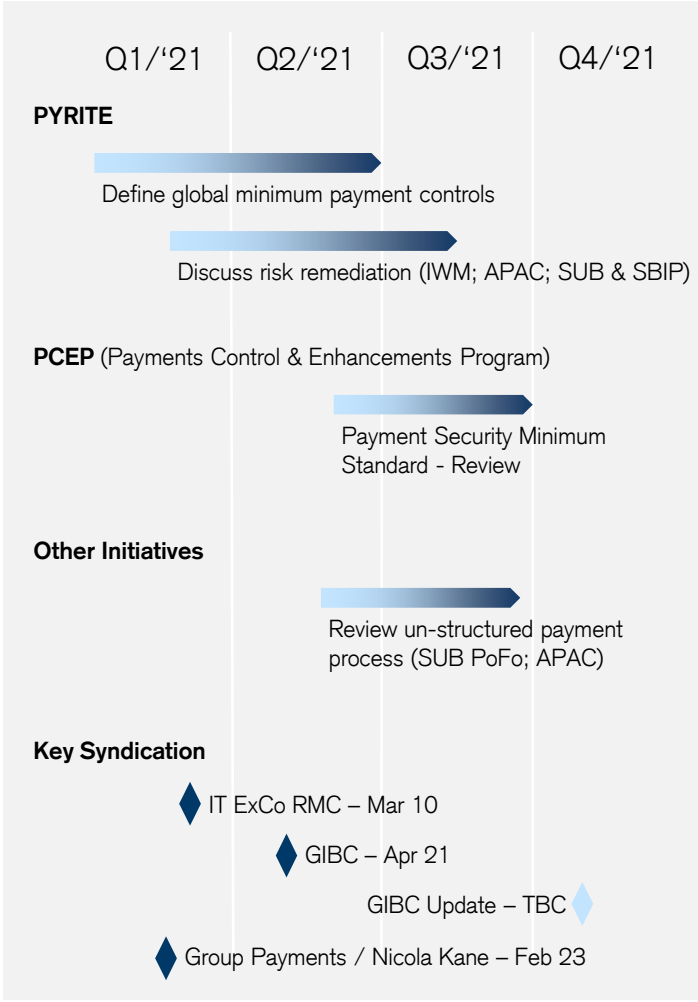
- The combination of technology risks and business / process risks is putting un-structured transactions at risk - and the risk is growing. Based on available technologies to potentially support transaction authentication, options should be evaluated to remediate the risks.

Source:
* = "A Guidance Framework for Selecting User Authentication Solutions" 8 November 2017 – Gartner

Follow-up actions – Status as of August

Getting connected with group wide initiatives to address the risk

Requirement	Implication
Reduce usage of in-secure payment channels: Reduce usage of un-structured and in-secure payment channels (e.g. e-mail; physical mail; SMS; fax)	Onboard all clients to the CS provided and secured platforms (e.g. CS Digital; CS Direct / CSX)
Validate un-structured payments: When accepting un-structured payments ensure appropriate security controls are in place (e.g. technology based authentication; transaction signing) for validation of the data.	Ensure security controls for authentication of the client (e.g. transaction signing; out of band confirmation)
Secure in-secure channels: In situations where the use of secure channels are not possible, ensure appropriate compensating controls are inplace. In-secure channels should be risk assessed and risk approved periodically or upon major changes impacting security controls.	Transmit sensitive data only via secured channels or channels with compensating controls (e.g. varying identification keys / tokens).



Requirement	Implication	Addressed by Actions per Division (key contacts): APAC	IWM	SUB	AM	IB
#1 - Reduce usage of in-secure payment channels: Reduce usage of un-structured and in-secure payment channels (e.g. e-mail; physical mail; SMS; fax)	Onboard all clients to the CS provided and secured platforms (e.g. CS Digital; CS Direct / CSX)		▪ xx ▪ xxx	▪ xx		▪ xx
Risk Coverage by listed actions (CISO view):		▪ Not applicable*	▪ Fully covered	▪ Partially covered	▪ TBC**	▪ Fully covered
#2 - Validate un-structured payments: When accepting un-structured payments ensure appropriate security controls are in place (e.g. technology based authentication; transaction signing) for validation of the data.	Ensure security controls for authentication of the client (e.g. transaction signing; out of band confirmation)	▪ xx ▪ xx	▪ xx ▪ xx		▪ xx	▪ xx
Risk Coverage by listed actions (CISO view):		▪ Partially covered	▪ Partially covered	▪ Partially covered	▪ Partially covered	▪ Partially covered
#3 - Secure in-secure channels: In situations where the use of secure channels are not possible, ensure appropriate compensating controls are inplace. In-secure channels (external accessible or CS internal channels) should be risk assessed and risk approved periodically or upon major changes impacting security controls.	Transmit sensitive data only via secured channels or channels with compensating controls (e.g. varying identification keys / tokens).	▪ xx ▪ xx	▪ xx	▪ xx	▪ xx	▪ xx
Risk Coverage by listed actions (CISO view):		▪ Fully covered	▪ Fully covered	▪ Partially covered	▪ Fully covered	▪ Fully covered

* = No electronic payment functionality offered in APAC
** = to be confirmed based on identified use cases (part of requirement #2)