Fighting Financial Fraud Together ›

› Alon Cohen

nsknox

By Way of Introduction

nsKnox (2016)	Intezer (2016)	Muvix (2015)	FilesX (2004) (Sold to IBM)	CyberArk (1999) (Nasdaq: CYBR)
FinSec	Cyber	M&E	Data Storage	Cyber

The Big-Bang of Technology

seeking stability in the aftermath

nsknox

The Technology Chaos

A flood of continually
Introduced new technologies

The Security Chaos

The cloud, frequent technology updates, growing technological complexities, global connectivity, high employee turnover

nsknox

The Regulatory Chaos

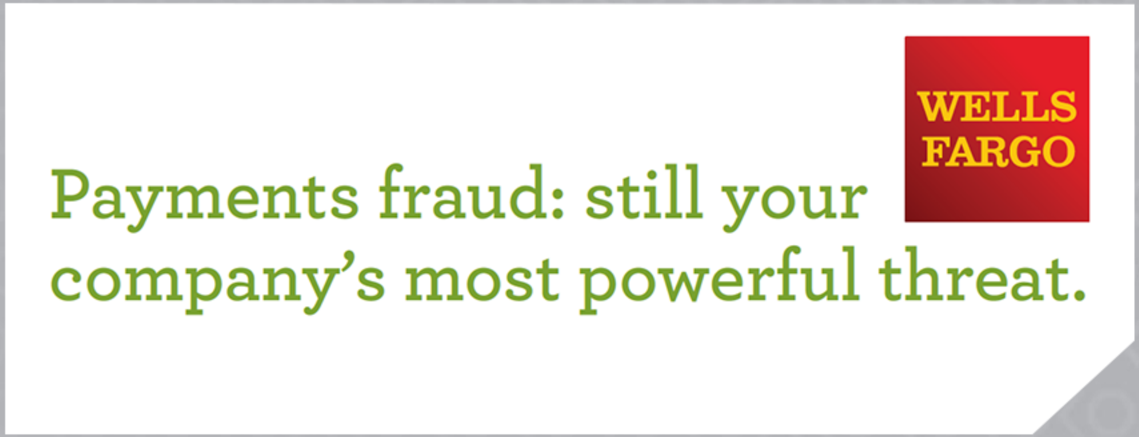
Regulations can’t keep up with ever changing needs

Organizations are constantly battling

cyber fraud attacks

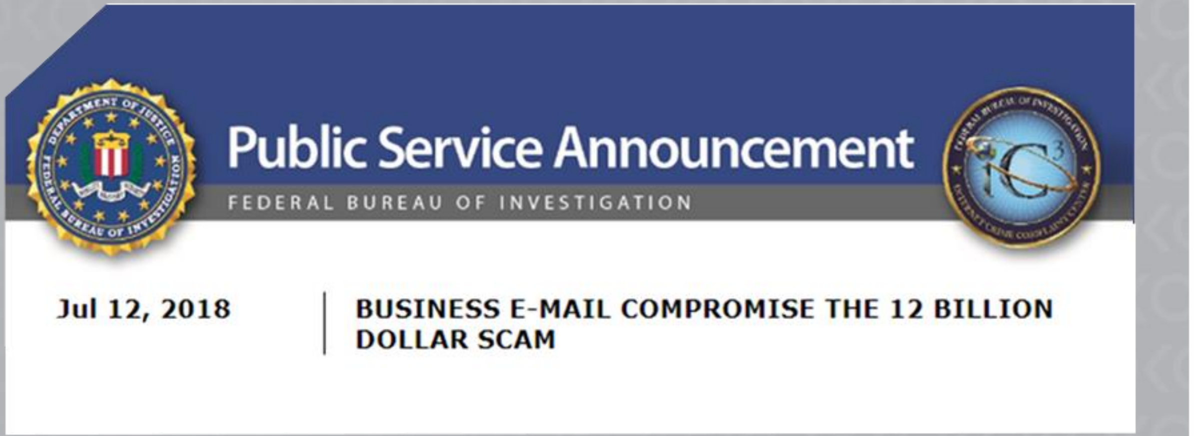
nsknox

The Rate of Attack & Losses are Growing



WELLS FARGO

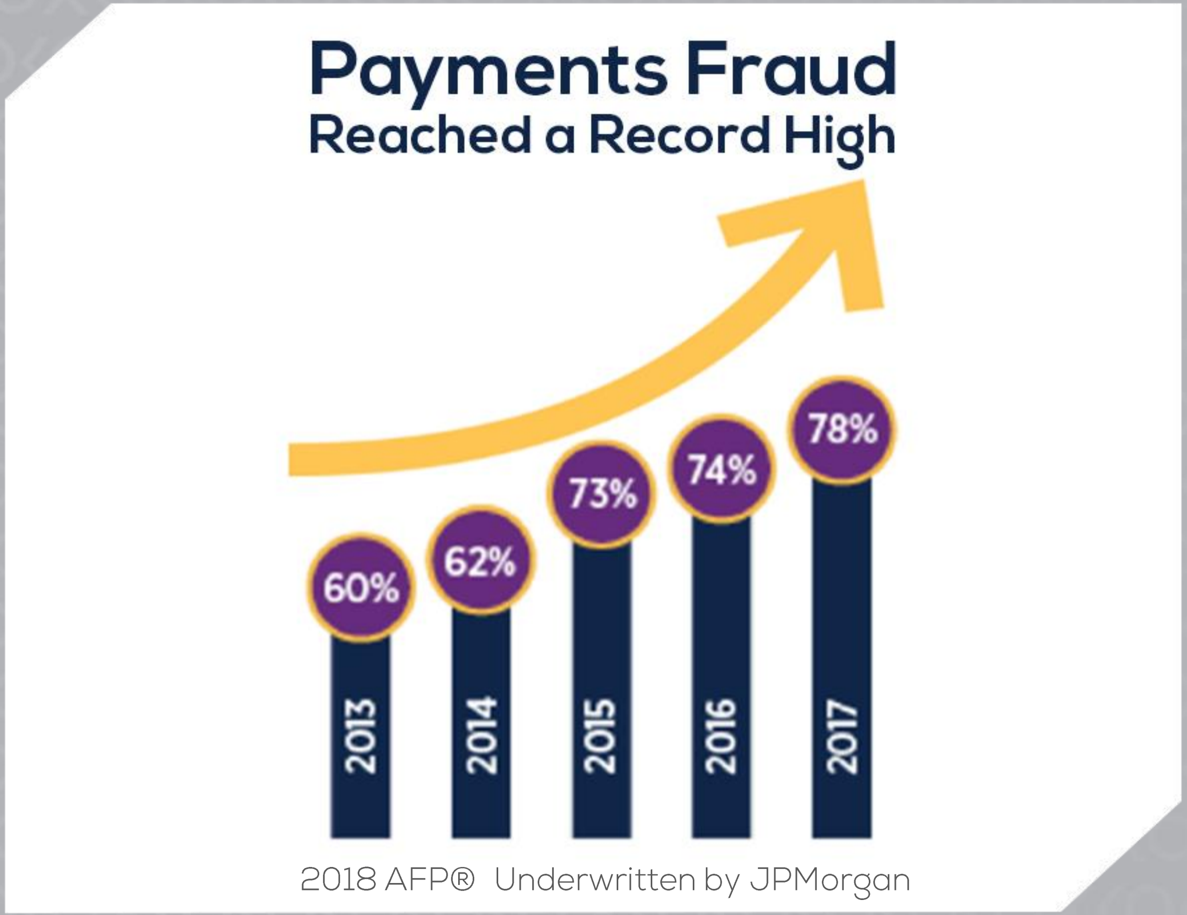
Payments fraud: still your company's most powerful threat.



Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

Jul 12, 2018 | BUSINESS E-MAIL COMPROMISE THE 12 BILLION DOLLAR SCAM

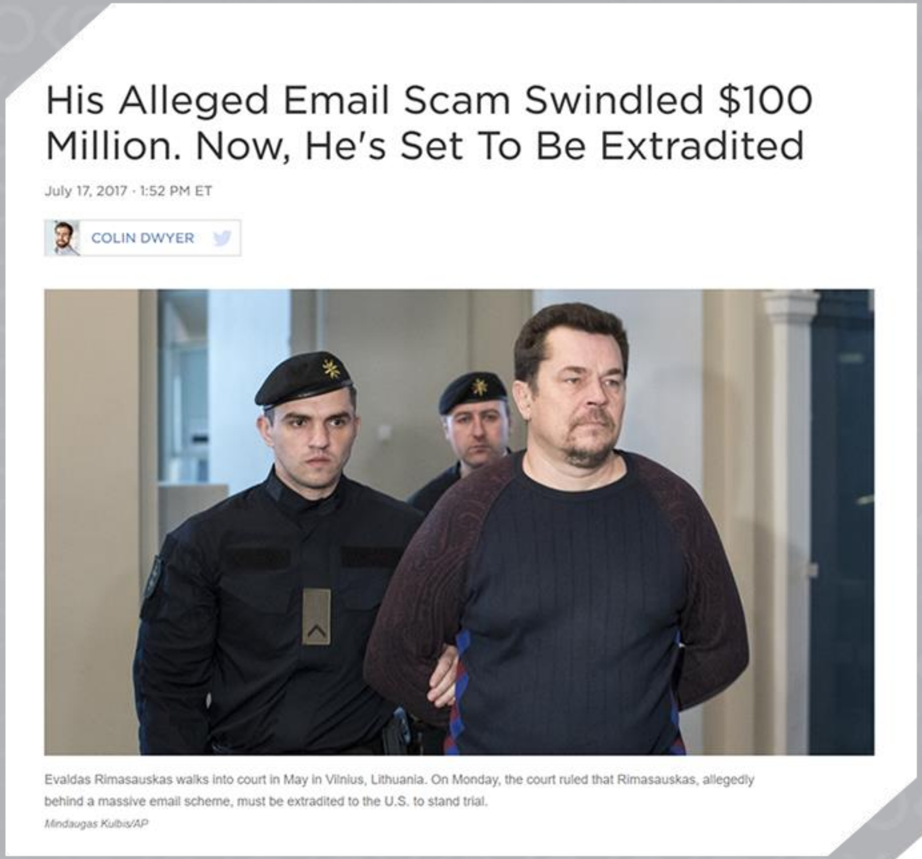


Payments Fraud

Reached a Record High

2018 AFP® Underwritten by JPMorgan

Cyber Fraud via Social Engineering: The Case of Evaldas Rimasauskas



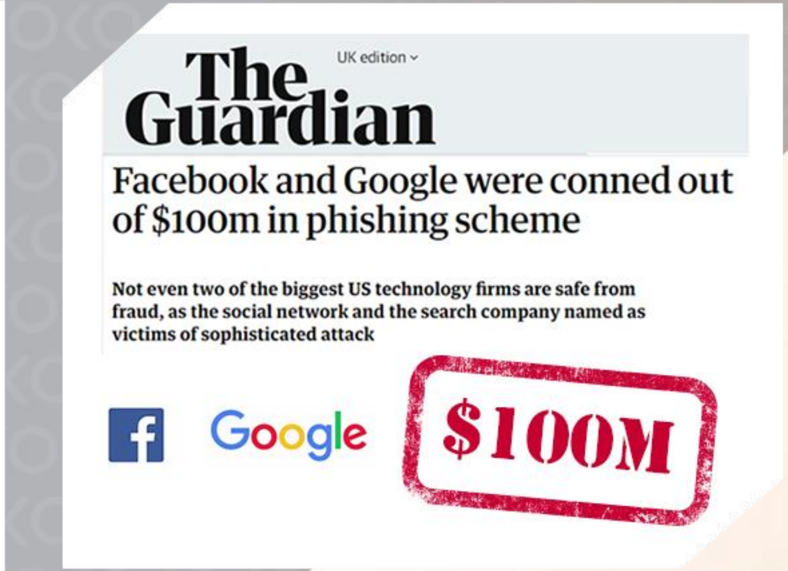
His Alleged Email Scam Swindled $100 Million. Now, He's Set To Be Extradited

July 17, 2017 · 1:52 PM ET

COLIN DWYER

Evaldas Rimasauskas walks into court in May in Vilnius, Lithuania. On Monday, the court ruled that Rimasauskas, allegedly behind a massive email scheme, must be extradited to the U.S. to stand trial.

Mindaugas Kulbis/AP



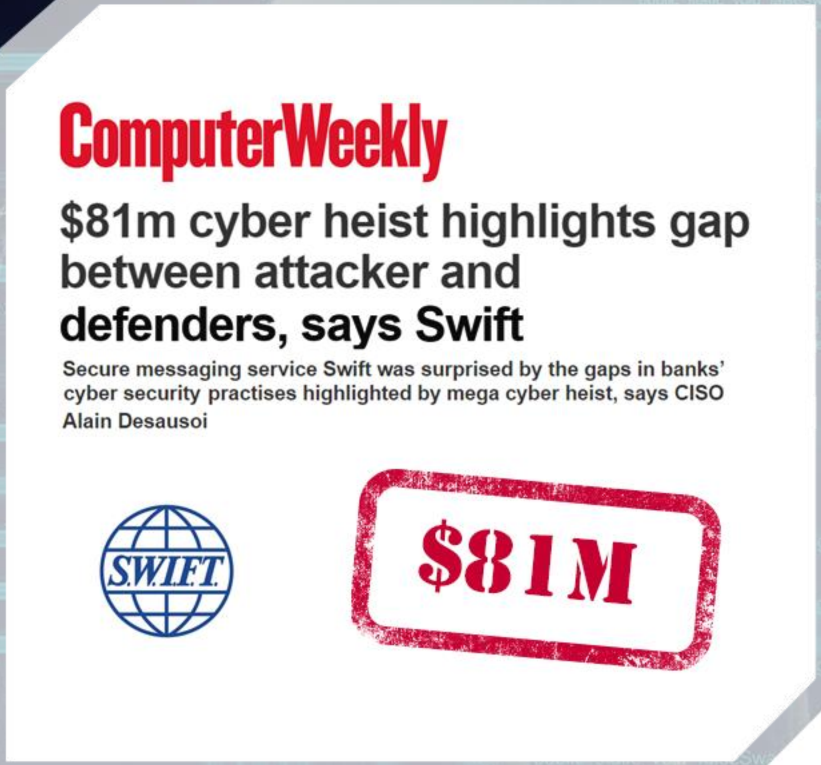
UK edition

The Guardian

Facebook and Google were conned out of $100m in phishing scheme

Not even two of the biggest US technology firms are safe from fraud, as the social network and the search company named as victims of sophisticated attack

Cyber Fraud via Infrastructure Manipulation: **The Case of SWIFT**



ComputerWeekly

$81m cyber heist highlights gap between attacker and defenders, says Swift

Secure messaging service Swift was surprised by the gaps in banks' cyber security practises highlighted by mega cyber heist, says CISO Alain Desausoi

SWIFT

$81M

nsknox

The Types of Cyber Fraud Are Many

FALSE INVOICE

CYBER ATTACK

VENDOR IMPERSONATIONS

INSIDER FRAUD

SOCIAL ENGINEERING

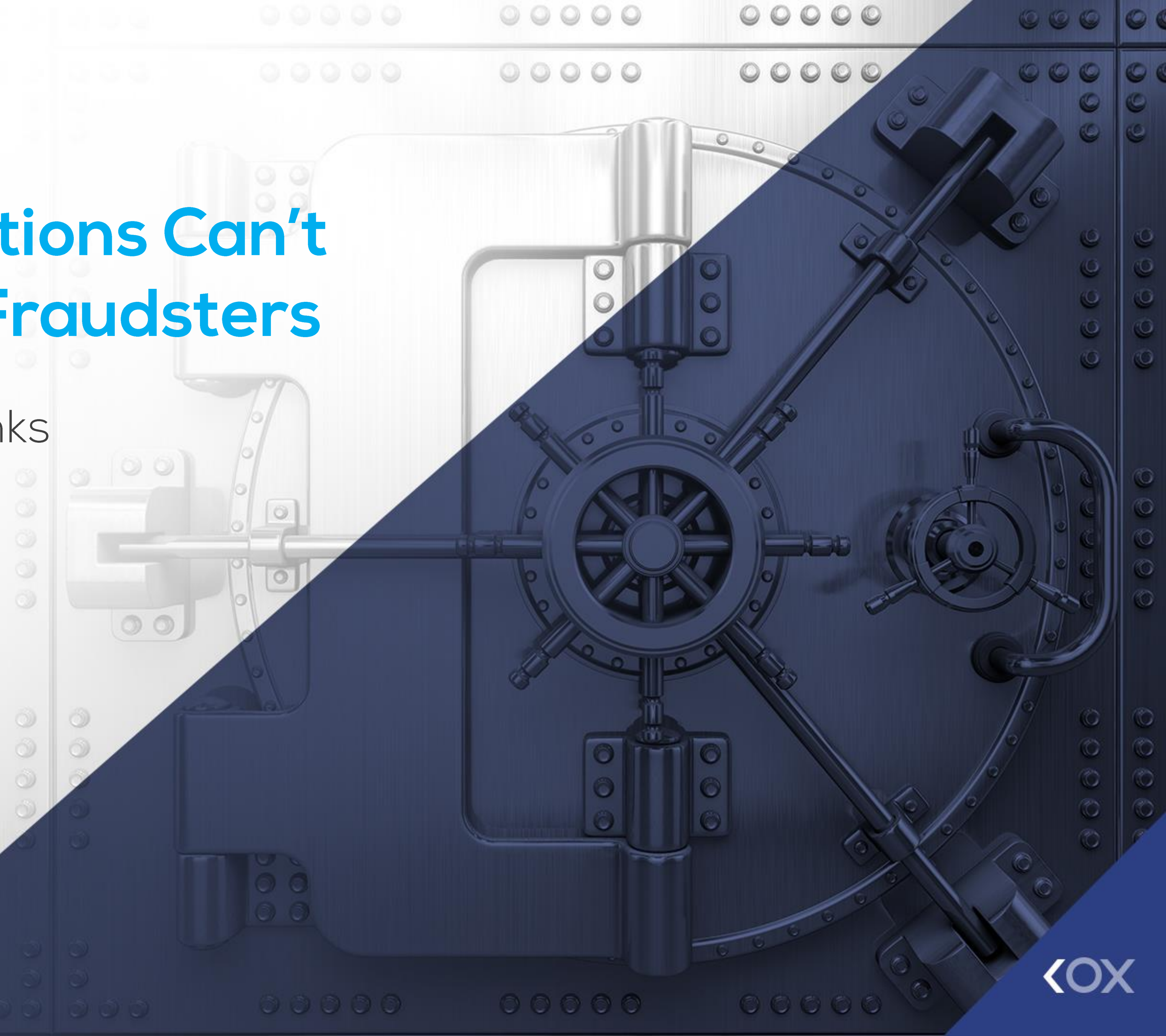
EAC Email Account Compromise

BEC Business Email Compromise

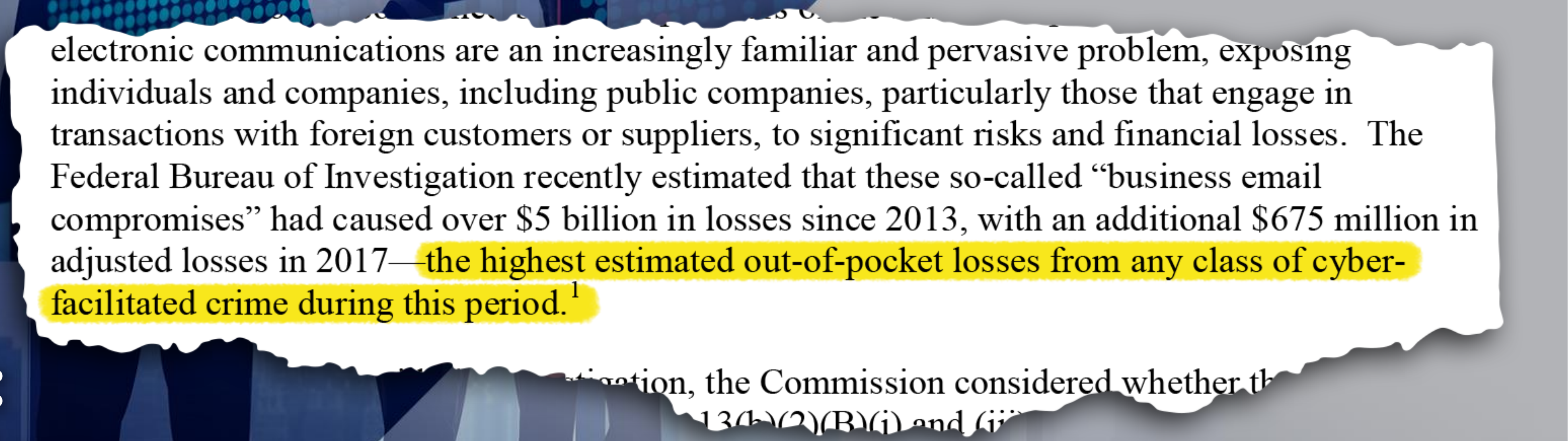
HUMAN ERROR

Current Fraud Solutions Can’t Keep Up With The Fraudsters

- Enterprises trust their banks for their protection
- Banks lack the required information about our business and our payees’ business



Even The SEC Has Ruled: Organizations Must Act



electronic communications are an increasingly familiar and pervasive problem, exposing individuals and companies, including public companies, particularly those that engage in transactions with foreign customers or suppliers, to significant risks and financial losses. The Federal Bureau of Investigation recently estimated that these so-called "business email compromises" had caused over $5 billion in losses since 2013, with an additional $675 million in adjusted losses in 2017—the highest estimated out-of-pocket losses from any class of cyber-facilitated crime during this period.[1]

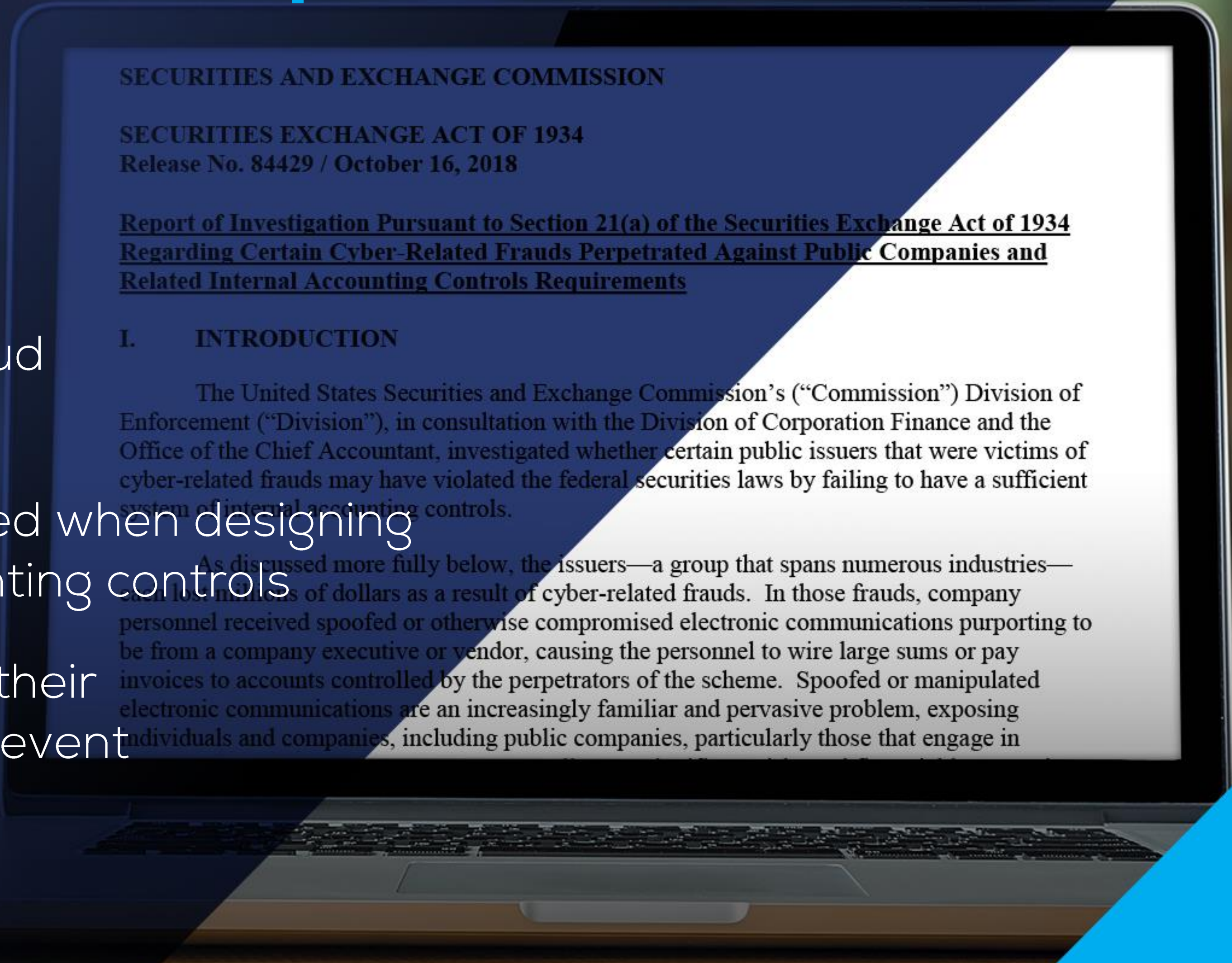
tigation, the Commission considered whether th
13(b)(2)(B)(i) and (ii)

nsknox

The SEC Investigative Report

Issued in October 2018

- 9 companies, with losses at tens of millions of dollars, investigated
- “Business Email Compromise” fraud is considered a serious threat
- Such threats need to be considered when designing and implementing internal accounting controls
- All companies need to verify that their procedures and controls would prevent losses



SECURITIES AND EXCHANGE COMMISSION

SECURITIES EXCHANGE ACT OF 1934
Release No. 84429 / October 16, 2018

Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934 Regarding Certain Cyber-Related Frauds Perpetrated Against Public Companies and Related Internal Accounting Controls Requirements

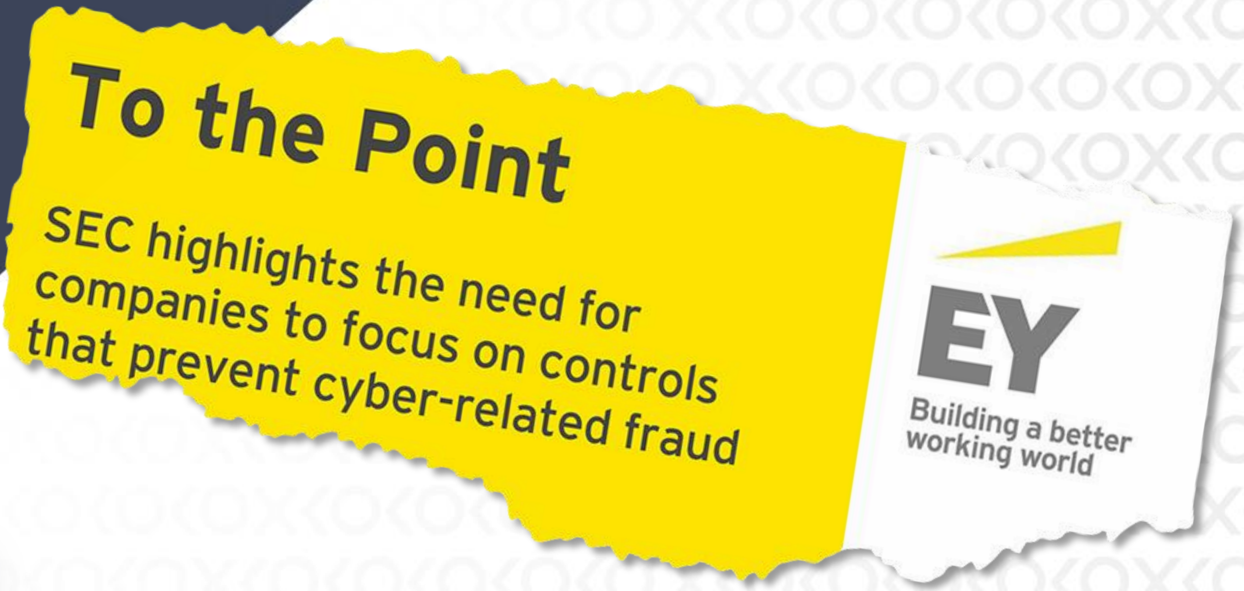
I. INTRODUCTION

The United States Securities and Exchange Commission’s (“Commission”) Division of Enforcement (“Division”), in consultation with the Division of Corporation Finance and the Office of the Chief Accountant, investigated whether certain public issuers that were victims of cyber-related frauds may have violated the federal securities laws by failing to have a sufficient system of internal accounting controls.

As discussed more fully below, the issuers—a group that spans numerous industries—each lost millions of dollars as a result of cyber-related frauds. In those frauds, company personnel received spoofed or otherwise compromised electronic communications purporting to be from a company executive or vendor, causing the personnel to wire large sums or pay invoices to accounts controlled by the perpetrators of the scheme. Spoofed or manipulated electronic communications are an increasingly familiar and pervasive problem, exposing individuals and companies, including public companies, particularly those that engage in

EY

31 October 2018



To the Point

SEC highlights the need for companies to focus on controls that prevent cyber-related fraud

EY

Building a better working world

> “Entities may need to revisit their controls related to the authorization of the transfer of funds and changes to vendor master file data…”

10 Must Have's

for Every Auditor in Fighting Payments Fraud

nsknox

#1 Must Have

Ensuring that payment security is on the CISO's priority list

Cyber-Grade Verification of All Payment Information & Communication

All payment information, either local or received via email, phone or fax are never trusted w/o cyber-grade authentication and verification

#2 Must Have

#3 Must Have

Real-Time End-to-End Controls

All payment data, requests and authorizations are verified in real time, at each step of the transaction journey.

nsknox

Centralized & Independent Controls

for all payment-related processes.

#4 Must Have

nsknox

#5 Must Have

A comprehensive and enforceable list of payment policies

where requests that don’t accord are automatically routed for explicit approval.

nsknox

Maximum payment thresholds for vendors

which trigger automatic blocking or explicit approval of transactions that exceed them.

nsknox

#6 Must Have

#7 Must Have

Cyber-Grade KYC Process

in supplier onboarding

nsknox

Requests for changes
to vendor master file data

to be automatically routed in real time for an independent verification w/ an authorized vendor representative.

#8 Must Have

nsknox

#9 Must Have

Prohibiting Out-of-Band payments at all-levels.

nsknox

No Single-Point Of Failure Across The Enterprise

Including executives, finance and IT

#10 Must Have

nsknox

TxAuthority™

The Weapon of Choice in the War on Cyber Fraud

nsknox

Corporate Payments Protection

with real-time detection and protection

› 1 Detects and prevents broad majority of fraud attempt types

› 2 Secures transactions with the approved supplier and account

› 3 Analyzes all data at every point in transaction journey

› 4 Easy installation with AP/AR operational efficiency

› 5 Helps ensure SOX & SEC compliance and D&O Liability

› 6 Ensures no single point-of-failure

nsknox