Bankers Association of Trinidad & Tobago (BATT)

(Interbank Anti-Fraud & Security Committee)

'Strategies for Fraud Detection & Prevention'

Presenter (s)- Antonio Ventour, Yanda Cox,

June 2017

Objective

At the end of this presentation, participants should be better able to:

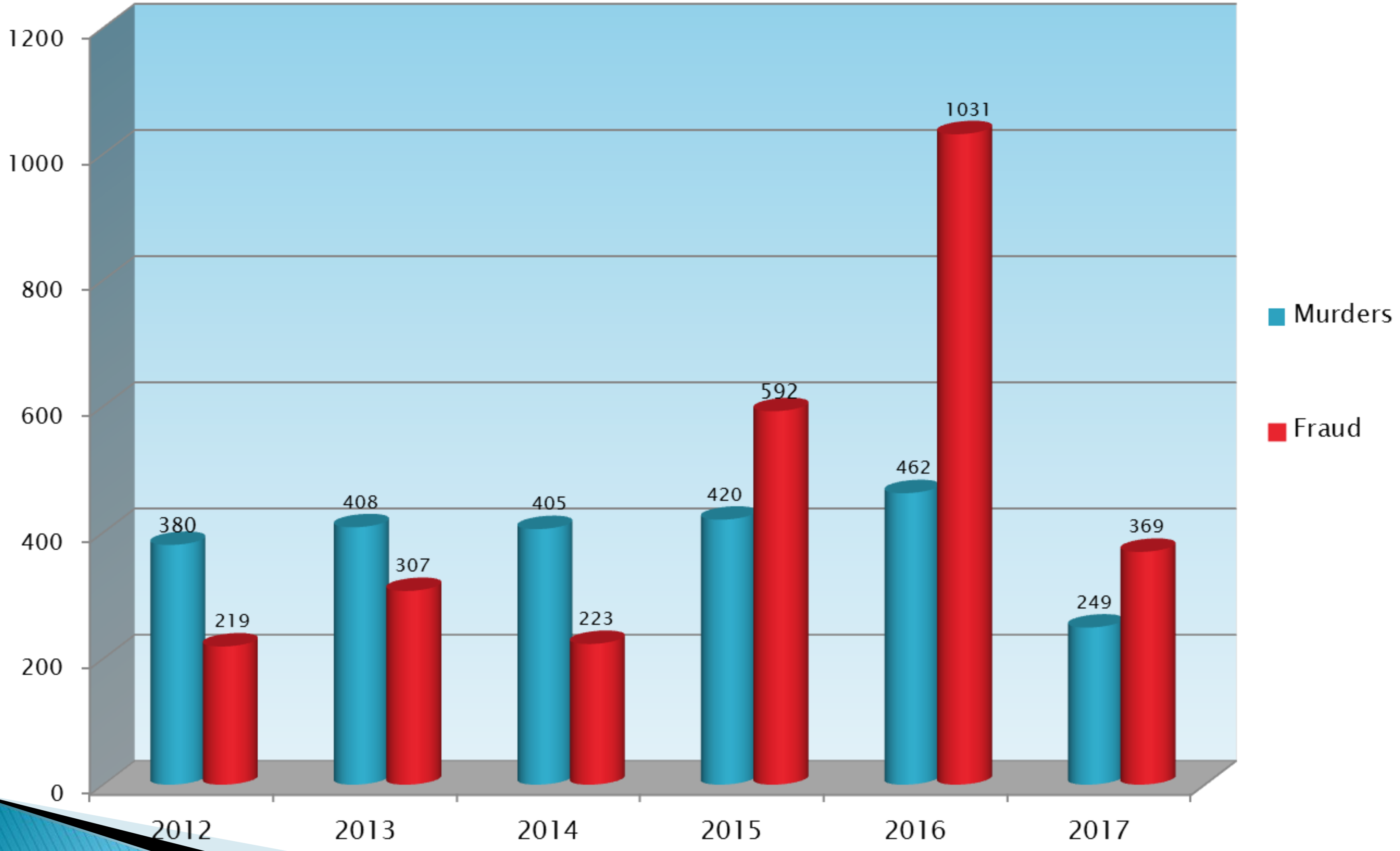
"Apply the appropriate skills and tools to more effectively detect and reduce the risk of fraud and fraud related activity in your day to day operations".

Learning Objectives

- Fraud Risk associated with Payment Channels
- Educate as to how certain fraud typologies can affect you and your business
- To recognize fraud (internally and externally) as an operational risk in an organization.
- The holistic approach to Detecting & Preventing the risk of fraud.
- Designing your Anti-Fraud Policy

Fraud, fraud and more fraud!

MURDERS vs FRAUD OFFENCES 2012-2017



Fraud Challenge

BANKERS ASSOCIATION OF TRINIDAD AND TOBAGO

You cannot prevent yourself from being "Targeted" by fraudsters…

- *you own a business*
- *you have or do not have a bank AC*
- *You have needs (fraudsters will satisfy the need)*
- *you have "no money"…you are still targeted (money mule/runner/ fronting)*

*…but, guess what!!...you **do not** have to be a "Victim"*

Fraud Challenge

- *…the human element aspect of any process/procedure is usually the weakest link in that process/procedure…*

Payment Channels (Internal & External Risk)

- Cash
- Cheques (manager's cheque)
- Card
- Wire Transfers (Online/Mobile Banking)

Cash Payment

Who Commits Fraud?

- **20% of all Employees are honest**
- **Another 20% of Employees are dishonest**
- **The other 60% would be dishonest if given the opportunity**
- **Up to 80% therefore is potentially dishonest.**

  (Study by Criminologist)

Occupational Fraud

This is defined as……

- “The use of one’s occupation for personal enrichment through the deliberate misuse or misapplication of employing organisation’s resources and assets”.

Cash – Related Risk

Internal Factors

- Embezzlement (taking the cash before it is registered into the business)
- Larceny (theft – taking the cash after it is registered into the business)

The Fix

Develop Procedures for Cash Processing Aspect of Business

- Segregation of duties (balancing/making up deposits)

- Independent verification (discrepancy investigation by another body)

2. Learn to recognise counterfeit currency (train staff)

Tips To Note In Detecting Counterfeit Bills

Security Features:

- Inferior coloration
- Waxy/smooth surface
- No security thread
- Absence of UV features
- Inferior paper
- Bills bearing the same serial number
- Images/Portrait not clear

Tips

- Know your money (http://www.central-bank.org.tt/know-your-money)

Site Informs of:

- The TT Notes/Bills in Circulation
- How the notes are produced and material
- How to Authenticate/Compare Notes

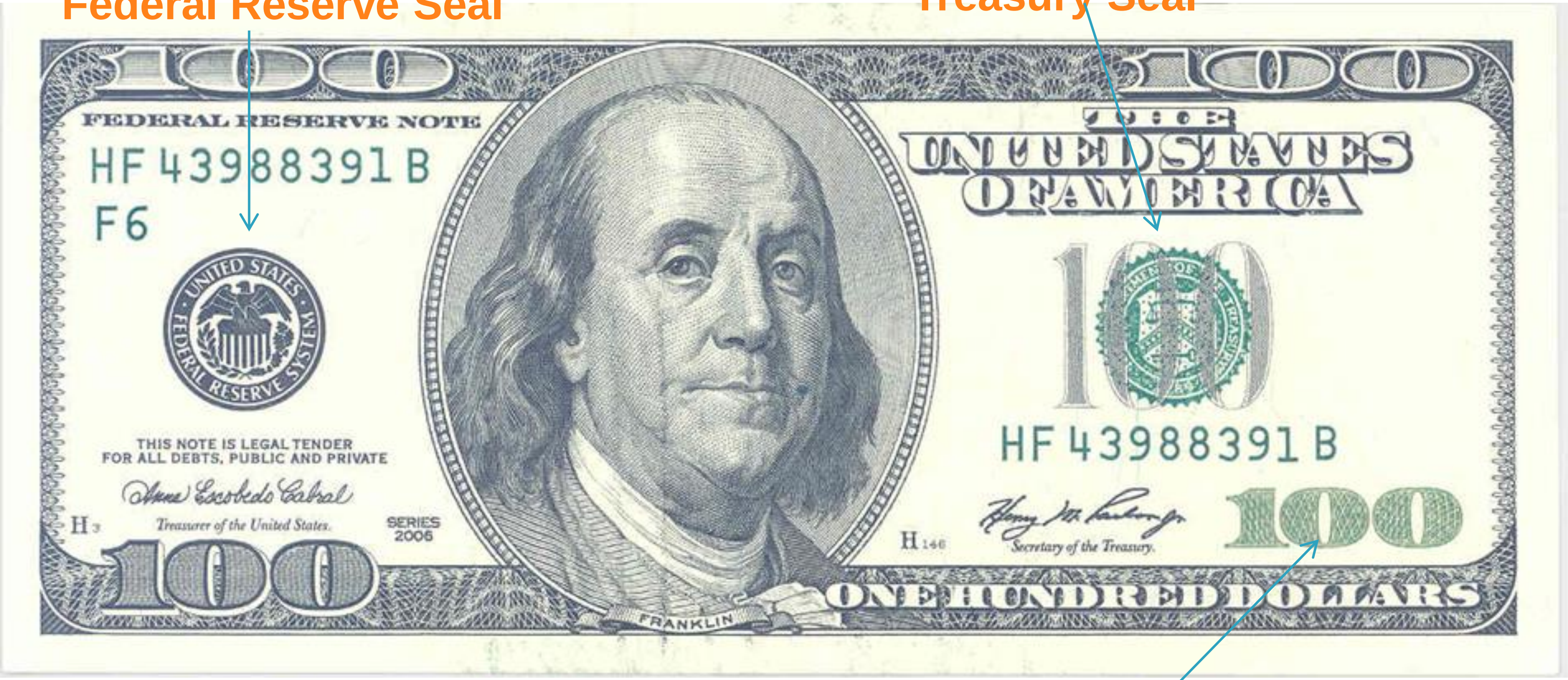
The Fix

- Conduct staff training/awareness sessions

Types of USD Currency

(security features)

BANKERS
ASSOCIATION
OF TRINIDAD AND TOBAGO


100
FEDERAL RESERVE NOTE
HF 43988391 B
F 6
UNITED STATES FEDERAL RESERVE SYSTEM
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
SERIES 2006
H 3
FRANKLIN
THE UNITED STATES OF AMERICA
HF 43988391 B
Secretary of the Treasury.
H 146
ONE HUNDRED DOLLARS

Federal Reserve Seal

Treasury Seal

Colour Shifting Ink

Green to Black

Types of USD Currency

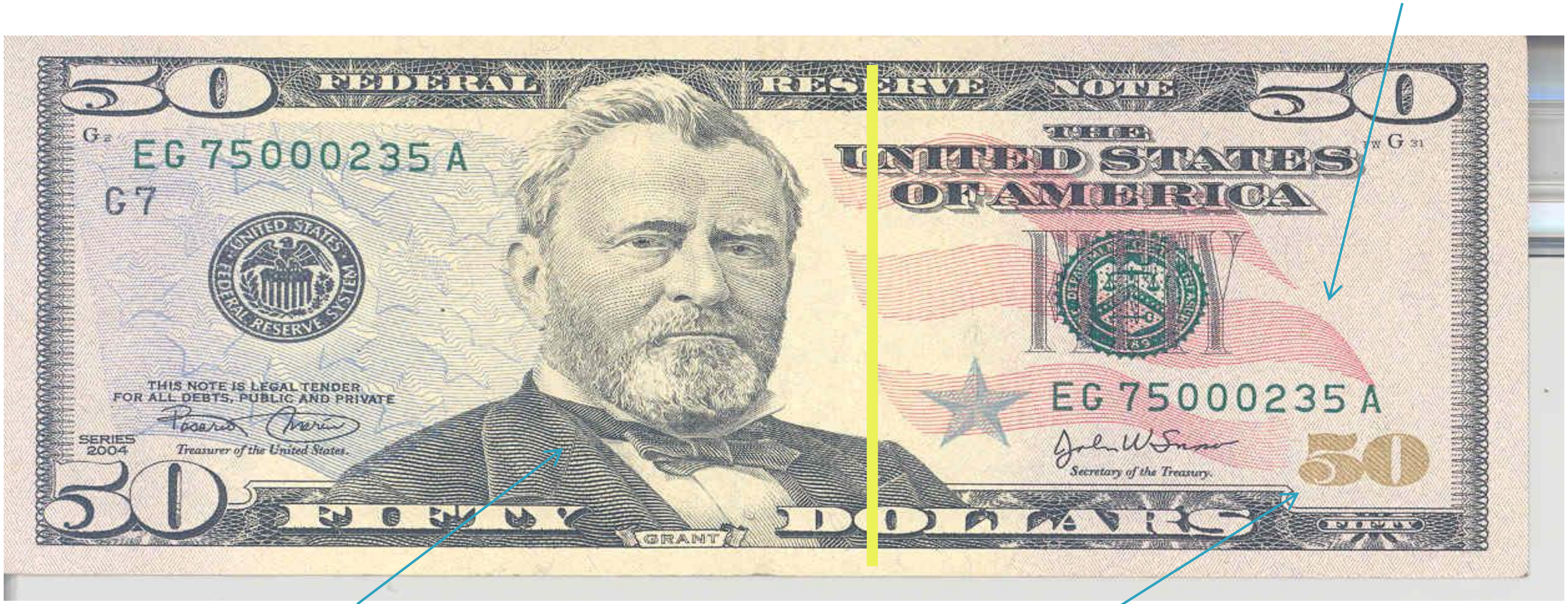
(Security Features)

PAPER: ¼ linen & ¾ cotton, red & blue fibers

SECURITY THREAD

Glows Yellow; 50 USD & Flag

WATERMARK:
Part of paper



MICROPRINTING:

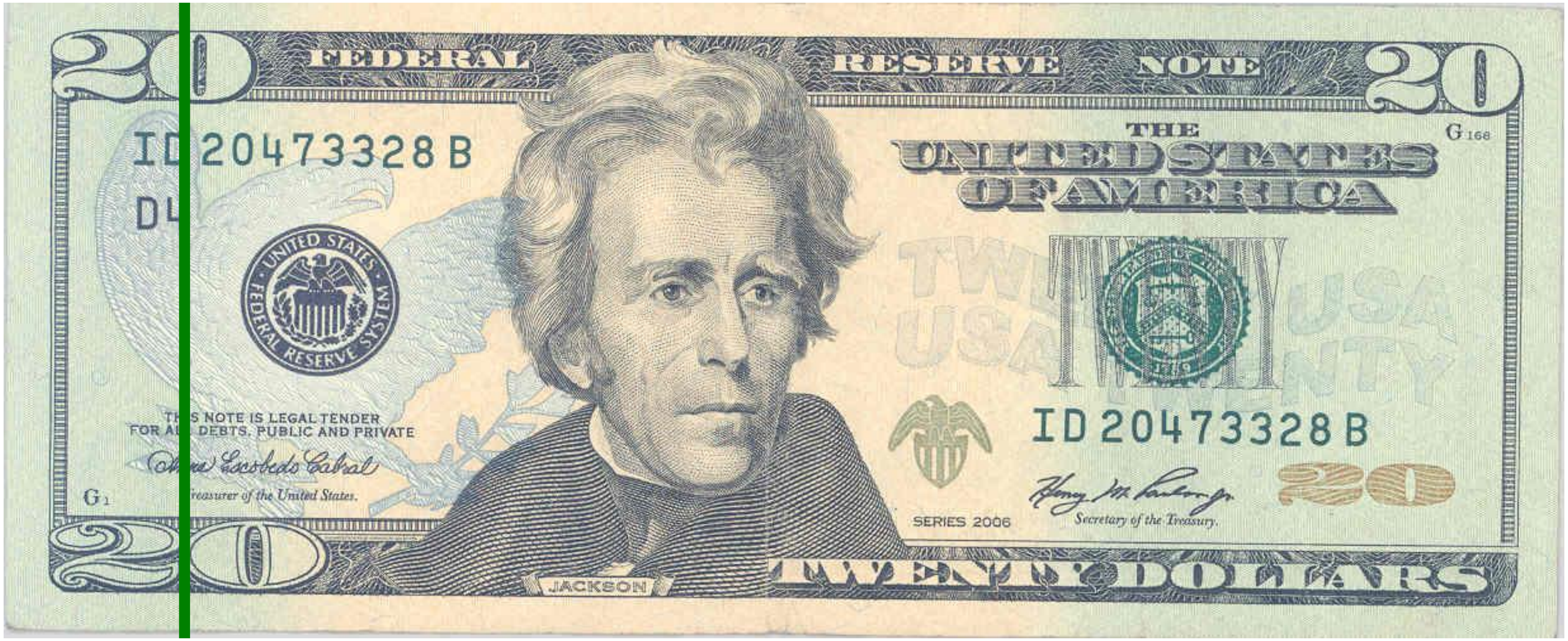
Along border and on stars

& on Grant's collar

Colour Shifting Ink

Copper – Green

Types of USD Currency
(Security Features)


FEDERAL RESERVE NOTE
THE UNITED STATES OF AMERICA
ID 20473328 B
D4
G1
G168
THIS NOTE IS LEGAL TENDER FOR ALL DEBTS, PUBLIC AND PRIVATE
Treasurer of the United States.
Secretary of the Treasury.
SERIES 2006
JACKSON
TWENTY DOLLARS
20
USA TWENTY

Fraud Typology – USD Currency

- Fraudster befriends social group
- Produce USD Bank Statement (to prove USD exist)
- Advise buyer – buy TTD manager’s cheque (want proof of payment)
- Do not release funds until in receipt of USD
- Send copy of Wire transfer from foreign bank to buyer
- Buyer release manager’s cheque to fraudster

Cheques

Cheque Fraud

Internal Factors:

Treat cheques like cash

- The Fix – Lock them away ; restrict/limit access)

Do not sign blank cheques leaves *(signature is your mandate)*

Accountant Helping Themselves *(a.k.a – Book Keeping Fraud)*

- The Fix – Reconcile AC as directed by Account Agreement *(reduces the risk of book keeping fraud)*

Cheque Fraud
Manager's Cheques

External Factor:

Do not release goods/services before verifying the authenticity of the cheque

- *Account Relationship Manager may be able to verify the cheque*
- *Verification may confirm if original cheque was negotiated already*
- *Date & Time cheque was purchased*

(The above is not a fool proof process)

Red Flag – Exercise caution when dealing with 'new clients' *(buying everything/items with significant prices*)

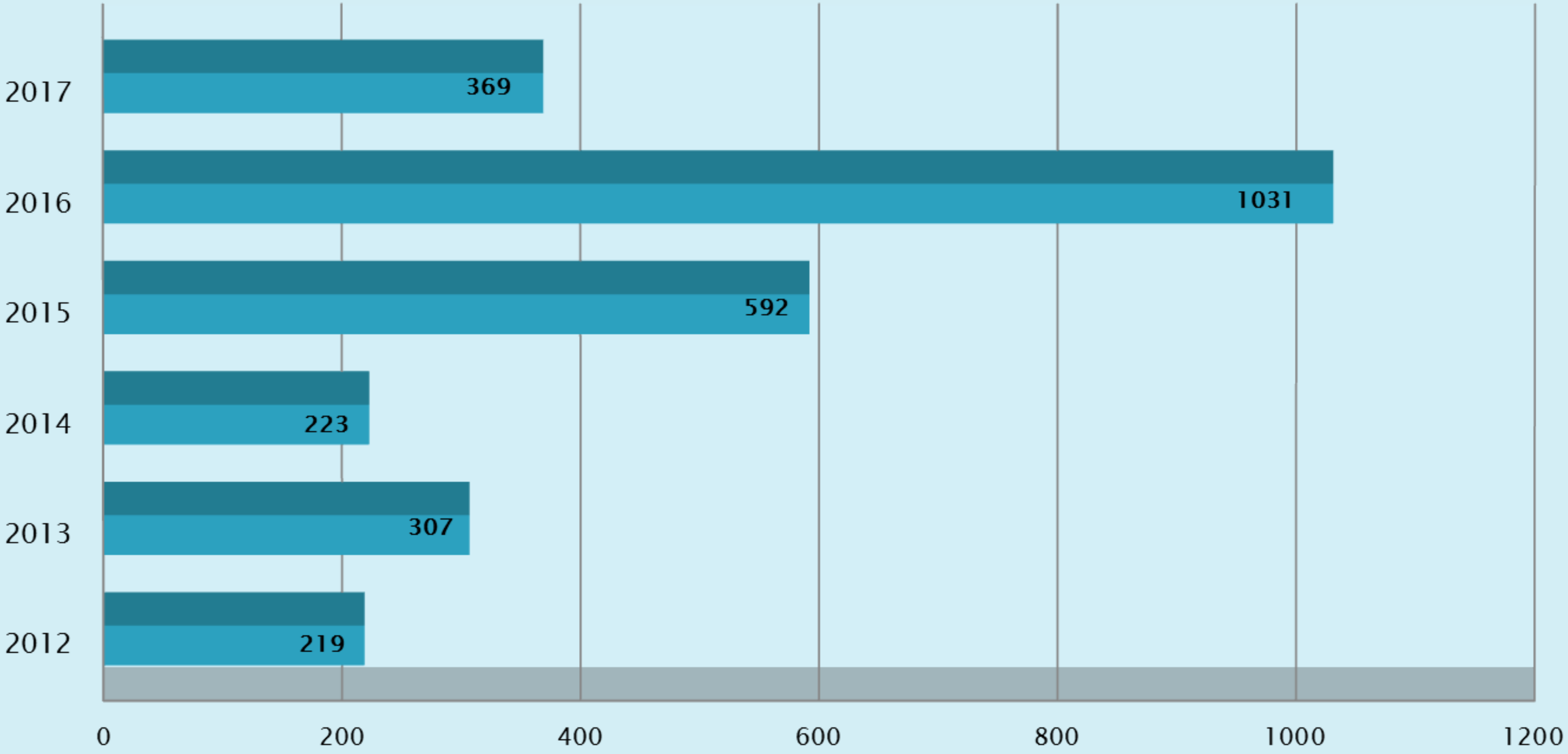
Cheque Fraud

- Look for the security features listed on the face of the cheque *(ALL manager's cheques have the features listed)*

- Look for the bleed through feature on the MICR line *(ALL manager's cheques have the bleed through)*

- Security features of manager's cheques include watermarks, MICR line (for clearing), synthetic fibres, bleed through MICR line *(some of these security features may not be present, if the cheque is scanned/photocopied and/or altered)*

Fraud Offences
2012–2017



Cards

Types of Card Fraud

- Skimming (ATM)
- Point of Sale (Merchant/POS)
- Lost/stolen cards
- Online Payments

Card Fraud – Skimming

What is Skimming

"*The surreptitious act of copying the encoded card information off the magnetic strip of either a credit or debit card with the intent to create a cloned card to facilitate fraudulent transactions on the legitimate account*"

(Source – BATT)

ATM Skimming

Skimming is an illegal activity that involves the installation of a device, usually undetectable by ATM users, that secretly records bank account data when the user inserts an ATM card into the machine. Criminals can then encode the stolen data onto a blank card and use it to loot the customer's bank account.

1 Hidden camera

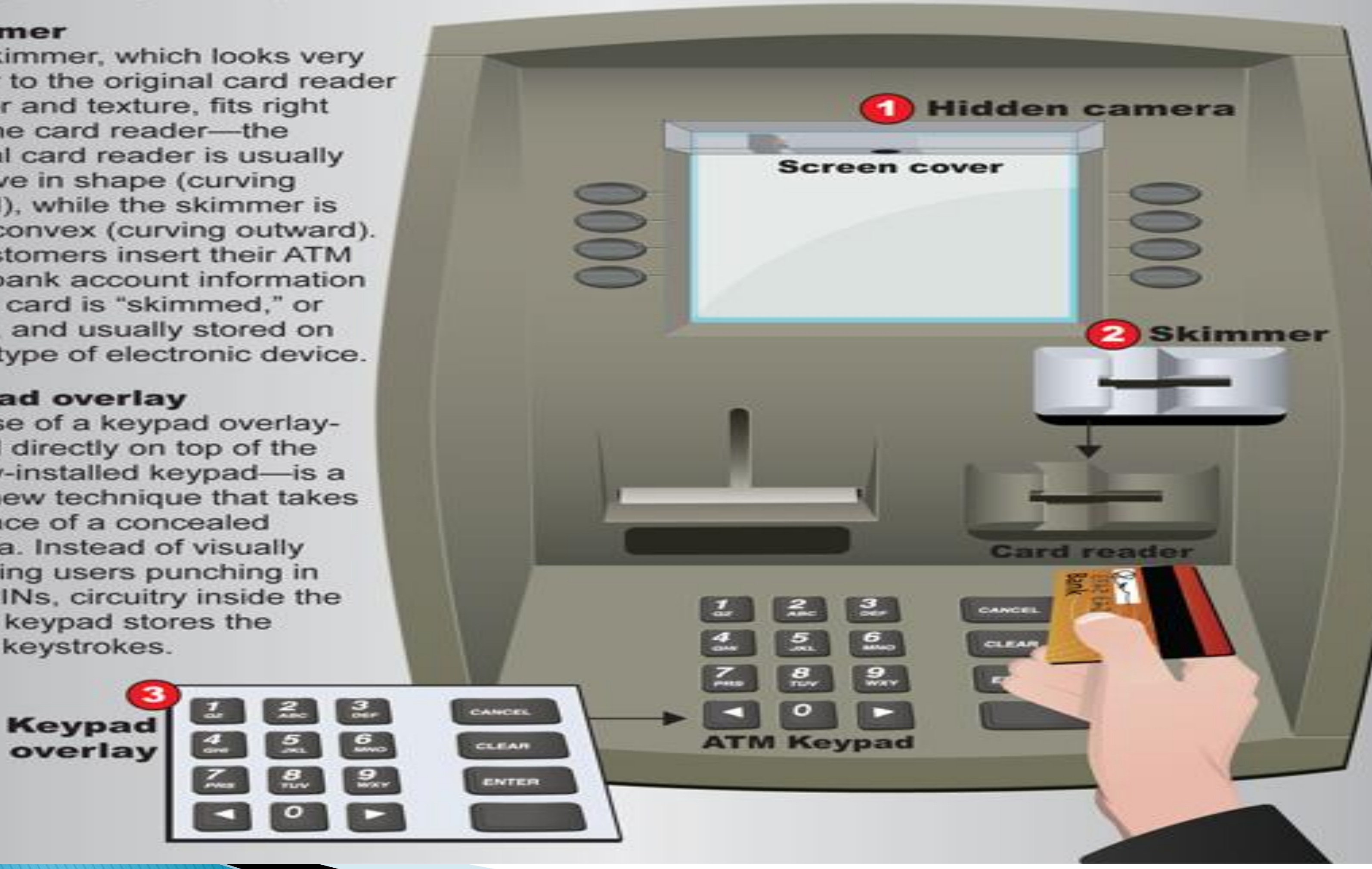
A concealed camera is typically used in conjunction with the skimming device in order to record customers typing their PIN into the ATM keypad. Cameras are usually concealed somewhere on the front of the ATM—in this example, just above the screen in a phony ATM part—or somewhere nearby (like a light fixture).

2 Skimmer

The skimmer, which looks very similar to the original card reader in color and texture, fits right over the card reader—the original card reader is usually concave in shape (curving inward), while the skimmer is more convex (curving outward). As customers insert their ATM card, bank account information on the card is "skimmed," or stolen, and usually stored on some type of electronic device.

3 Keypad overlay

The use of a keypad overlay-placed directly on top of the factory-installed keypad—is a fairly new technique that takes the place of a concealed camera. Instead of visually recording users punching in their PINs, circuitry inside the phony keypad stores the actual keystrokes.



Protect against skimming at ABM

ABM safety tips

- Always use your free hand to shield the numbers when entering your PIN.
- If PIN Shields are attached to the ATM – Use them as designed...do not lift flap.
- Beware of suspicious looking device/s.
- Be cautious about accepting assistance
- Never disclose your PIN to anyone.
- Look around before you approach the ABM, if anyone is watching you or standing too close, leave immediately and use another ABM.

15 Foreign Nationals Arrested – ATM

FRAUD SQUAD

(Between 26/1/16 – 28/06/17)

Female 1 ; Male 14

- Ecuador – 1
- Spain – 4
- England – 1
- Argentina – 1
- China – 2
- Bolivia – 1
- Canada – 1
- Bulgaria – 4

Skimming – Where & How

At the Cashier

- Hand held skimming device
- Cards are swiped unsuspecting of the customer using skimming device

MSR206

MSR905

Tips to detect Card Fraud

- Be wary of suspicious card holder behaviour
  - *More than one card to effect one purchase*
  - *Choosing goods randomly/ shopping in groups*
  - *Purchasing multiple high ticket items*
  - *Multiple foreign Cards in his/her possession*

- Compare the signature on the receipt, by holding on to the card, against the signature on the reverse of the card

- Beware of any signs of tampering.

Protect yourself from Credit/Debit Card Payment Fraud

- Never let your card out of your sight.
- If transacting any payment online, ensure that the site is secure.
- Beware of phishing sites.
- Always use your free hand to shield the numbers when entering your PIN

Card Fraud – Lost/Stolen Cards

Stolen Cards

- Cards are taken at the point of purchase
- Cards used without the consent of the card/account holder (domestic situation / friendly fraud)

Lost Cards

- Lost cards are used to assist with stolen card typology

- *Report lost/stolen cards to your bankers immediately*
- *Be aware of the bank's hotline numbers and reporting options for your bankers*

‘ KEEP AN HONEST MAN HONEST’

- Procedures
- Policy
- Supervision

Tips To Reduce risk (internal)

- Monitor payment area/workstation for skimmers/lost cards
- Educate/train your employees
- Examine your terminals (portable)
- Segregation of Duty

Wire Transfer

Wire Transfer Fraud

Wire Transfer Fraud can emanate from several fraud typologies:

- Social Engineering – *the art of manipulating people to secure personal and/or confidential/private information*
- Phishing – social engineering through emails that contain hyperlinks/attachments
- Malware/Viruses (browsing internet/rouge sites)
- Sharing your online credentials *(people you trust)*

Wire Transfer Fraud

- Transacting business on a compromised device (virus/malware)
- Business Email Compromise (BEC) (account take-over)

Business Email Compromise

- **Business Email Compromise** is a sophisticated scam targeting **businesses** working with foreign suppliers and/or **businesses** that regularly perform wire transfer payments.

- The fraudulent wire transfer payments sent to foreign banks may be transferred several times but are quickly dispersed.

Business Email Compromise

- According to the FBI – BEC is more sophisticated than any similar scam seen before.
- FACT: Total reported global losses from 2013 to 2016 – USD $2.3Billion in 79 countries
- Majority of the transfers are going to Asian banks located within China and Hong Kong.”

Business Email Compromise

- Begins with Email account compromise of high-level business executives (CEO)

- Fraudster sends a wire transfer request from the compromised account to a second employee within the company who is normally responsible for processing these requests.

- A request for a wire transfer is sometimes sent from the compromised account directly to the financial institution with instructions to urgently send funds to bank ‘X’ for reason ‘Y.'

- Fraudsters do their homework before targeting a business.

Business Email Compromise

Fraudulent Domain Typology

- Email employees or Financial Institution from a look-alike domain name that is one or two letters off from the target company's true domain name.

sample.com

sarnple.com

Victims of BEC

- Small businesses to large corporations.
- Fraudsters monitor and study their victims using social engineering techniques prior to initiating the BEC scam.
- Victims may also first receive “phishing” emails requesting additional details regarding the business or individual being targeted (name, travel dates, etc.).

Victims of BEC

- Some victims reported being a victim of various Ransomware cyber intrusions immediately preceding a BEC incident.

- Intrusions can initially be facilitated through a phishing scam in which a victim receives an email from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the fraudster(s) access to the victim's data, including passwords or financial account information.

Business Email Compromise – Scenario

- The accountant received an e-mail from her CEO, who at the time was on a business trip in China. The email instructed payment to one of their suppliers which was related to his business trip.
- The CEO said in the email that a Corporate Secretary (CS) will contact the accountant to provide further details.
- It was not unusual for the accountant to receive e-mails requesting a transfer of funds (payments) from the CEO

Scenario – Con't

- The accountant received an email purporting to be from the CS of the supplier related to the CEO's business trip with an appropriate letter of authorization attached "inclusive of CEO's signature over the company's seal".

- The email included instructions to wire USD$737,000 to a bank in China

- The next day, the CEO happened to call regarding another matter, the accountant mentioned that she had completed the wire transfer the day before

Scenario – Con’t

- The CEO said he had never sent the e-mail and knew nothing about any wire to China.

Tips To Assist In Managing – Online Threats

(it takes discipline & commitment…drop your bad habits)

- Encrypt emails that contain financial arrangements
- Develop and implement “Know Your Customer Policy – KYC” *(at both ends – customer & supplier)….inclusive of their financial history ; a contact number and contact person (by name and know their voice)*
- **Verification Call** *(call back process)– do not verify via emails)*

Online Fraud *(business email compromise – leading to wire transfer fraud*

KEY RED FLAGS

- Change in Account Number
- Change in Beneficiary Bank
- Change in Jurisdiction
- Email contact change

The Fix – To Avoid BEC

- VERIFY CHANGES in supplier/vendor payment location and confirm requests for transfer of funds *(employ Know Your Customer Policy)*

- Be wary of free, web-based e-mail accounts, which are more susceptible to being hacked *(know email address thoroughly)*

The Fix – Online Fraud – BEC

- DO NOT open spam email, click on links in the email, or open attachments in spam. These often contain malware that will give subjects access to your computer system. Delete spam.

- Consider using the Forward option instead of the Reply option to respond to any business emails. You can either type in the correct email address or select it from the email address book to ensure the intended recipient's correct email address is used.

- DO YOUR ONLINE BANKING FROM A SECURE DEVICE *(device designated to online banking transactions only)*

The Fix – To Reduce the Risk of Online Fraud

- Do not send private or financial information via an unsecured email address

- Use Encrypted email

- Do not access any online facility via an email
  - *"Don't be the weak link…Don't click on the hyperlink"*

    (Source – BATT Inter Bank Fraud Committee)
- Reconcile your account – in accordance with AC agreement.

What to do if you are a victim

BANKERS ASSOCIATION OF TRINIDAD AND TOBAGO

- Contact your financial institution immediately upon discovering the fraudulent transfer

- Your financial institution will render assistance in an attempt to recall the funds.

Website Safety Tips

Basic Online Security Tips

- Use (and protect) strong PINS and passwords (use phrases e.g "My dog is Dangerous*"; "2Meet@noon etc.)

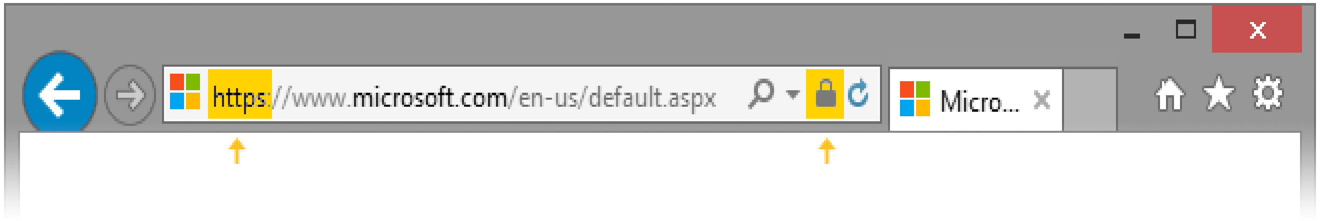
- Keep computer virus programmes updated with the latest programme

- **Confirm that the web address begins with HTTPS**

- If the URL in the address bar starts with HTTPS (instead of HTTP), the page is more secure. Never type passwords or other personal information unless you see the HTTPS

Look for a lock in the address bar

A lock icon in the address bar also indicates a more secure connection, which makes it harder for a hacker to view the information that you type.



https://www.microsoft.com/en-us/default.aspx

Facts About Cyber Threats

Cybercrime is expected to cost the world more than $6 trillion by 2021 (up from $3 trillion in 2015).

Projection by Cybercrime Experts

RANSOMEWARE

Cyberattack (‘WannaCry Ransomeware – May 2017)

- Ransomware is a type of malicious software that takes over a computer and locks the user out, preventing the user from accessing any files until they pay money.

- Friday, 5 May 17, a massive cyberattack hit approximately 200,000 victims in at least 150 countries including the UK, Japan and China. The cyberattack involved a ransomware called ‘WannaCry’.

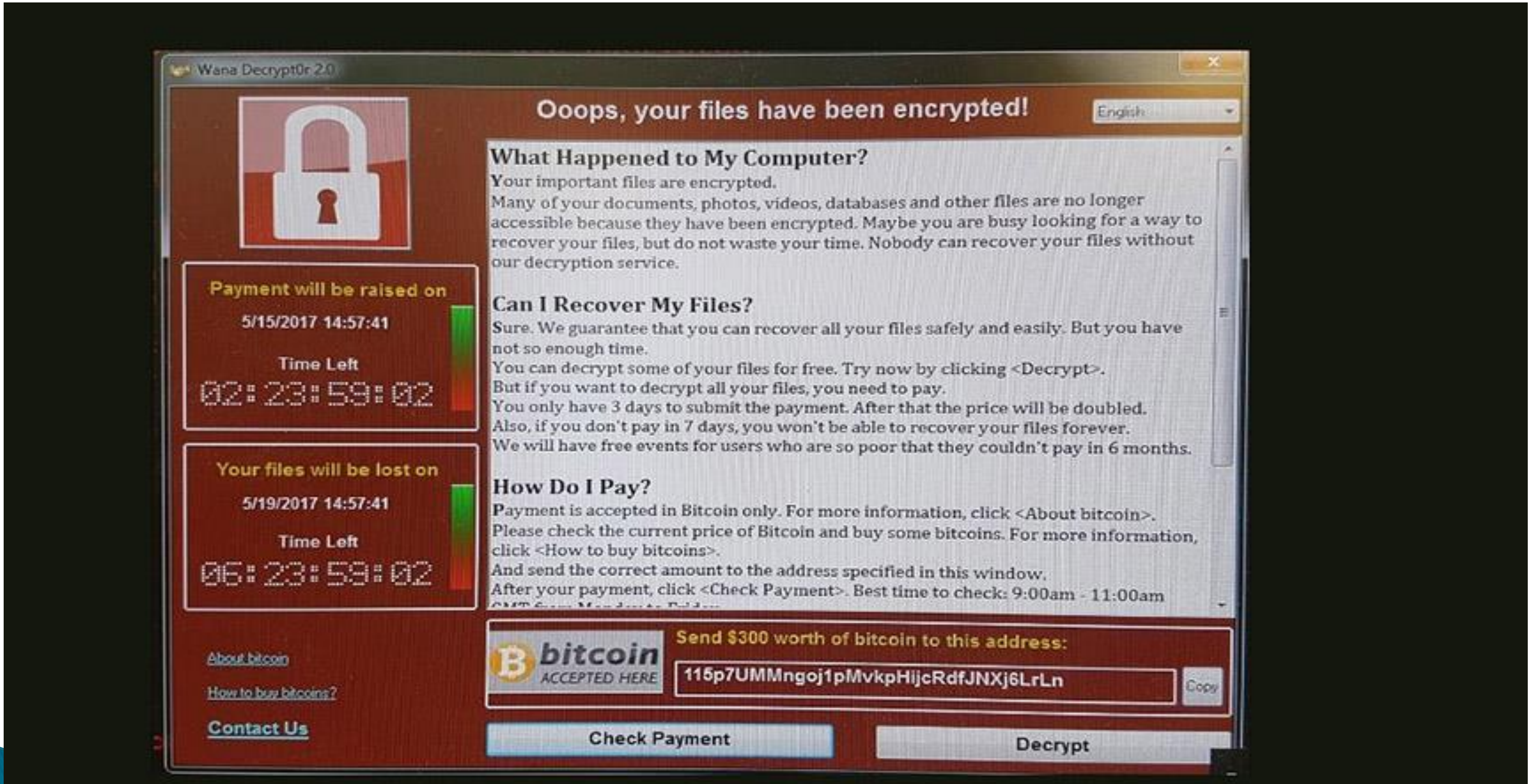
- Files on affected computers were encrypted. Users were instructed to pay a ransom with bitcoin to unscramble them. Payment demands ranged from $300 , threatening to data forever if the amount was not cleared in Bitcoin before the clock ran out.

- Several businesses and large organizations were affected including UK hospitals, a telecom and natural gas company in Spain, FedEx, the Russian Interior Ministry, Hitachi Ltd., and French auto maker Renault SA.

- The attack took advantage of security vulnerabilities in Microsoft Corp. software that was either too old to be supported by security patches or hadn’t been patched by users.

- The virus was slowed down by the identification and activation of a "kill switch" embedded in the virus’ code.

Lockscreen displayed by the WannaCry crypto-locking ransomware used in the attacks. ***(Source: Lawrence Dunhill)***



Ooops, your files have been encrypted!

Payment will be raised on

5/15/2017 14:57:41

Time Left

02:23:59:02

Your files will be lost on

5/19/2017 14:57:41

Time Left

06:23:59:02

About bitcoin

How to buy bitcoins?

Contact Us

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

bitcoin ACCEPTED HERE

Send $300 worth of bitcoin to this address:

115p7UMMngoj1pMvkpHijcRdfJNXj6LrLn

http://ransomware.databreachtoday.com

Ransomware Attacks

- The most common Ransomware basically encrypts and locks all content on a persons computer and requires a payment to be unlocked or decrypted.

- Director of the Centre of Computational Intelligence for Cyber Security at Unitec Auckland said “ransomware affected tens of thousands of people in 2016 and is estimated to have profited the criminals to the tune of US$1 billion.

Ransomware Attacks

- Hospitals, business and governments, no target is too big for today's sophisticated cyber criminals - it's costing US$445 billion per year globally.
- Hospitals became a major target raising serious concerns over patient data and privacy along with the threat of mass murder.
- In November 2016 three hospitals in England
- In May 2017 a Washington, D.C-area hospital chain was targeted . They were forced to revert to paper records

Protecting yourself from Ransomware (May 2017)

- Make sure your device's software is up to date. Software updates often contain lots of patches that fix bugs and close security loopholes; regularly using Windows Update or the Software Update feature on a Mac will help insulate you from problems. You can also set your devices to install those updates automatically.
- If you don't already have a backup routine, start now and regularly save copies of all your files.
- Use strong passwords (hard-to-break) passwords for each of your services.
- At work, check with your IT administrator to make sure your organization's devices are protected from WannaCry.
- Unexpected emails should be treated with caution as phishing is one of the most common types of attacks used by fraudsters to compromise machines.

Safest Tip of All

The name of the game is to:

VERIFY VERIFY VERIFY!!!!!!

- Pick Up The Phone
- Establish a Relationship with your supplier/Vendor
- Employ – KYC policy

Designing Your Anti-fraud Policy "Overview"

- The general content of the Anti-fraud policy
- An overview of the purpose of the Anti-Fraud policy
- The commitment to Fraud Prevention
- The objectives of the policy

Designing Your Anti-fraud Policy "Overview"

- Definition of Fraud Risk
- Examples of fraud
- Policy and Procedure Development
- References

Designing your Anti-fraud Policy

An overview of the purpose of the Anti-Fraud policy

- Customer service and trust is seriously damaged by fraud
- Fraud is a real threat to the finances of most organisations
- The end results of not effectively managing both internal and external fraud can be extensive

Designing Your Anti-fraud Policy

The commitment to Fraud Prevention

- The organisation’s commitment to ensuring that fraud or risk of fraud is reduced considerably
- The organisation will not tolerate any level of fraud or corruption committed by its employees
- All employees have a responsibility to report known or suspected incidents of fraud
- Any instance or suspected instance of internal or external fraud must be thoroughly investigated and dealt with appropriately.

Designing Your Anti-fraud Policy

BANKERS ASSOCIATION OF TRINIDAD AND TOBAGO

Objectives of the Anti-Fraud Policy

- To ensure that ALL persons (including Executives/Senior Management) understand their role and responsibilities in the prevention, detection and reporting of potential fraud issues
- Promote a proactive fraud prevention culture (includes training) for all employees
- Emphasize the organisation's position of zero tolerance with respect to internal fraud and the steps taken to manage external fraud
- Ensure the organisation complies with all applicable fraud-related regulatory requirements.

Designing Your Anti-Fraud Policy

BANKERS ASSOCIATION OF TRINIDAD AND TOBAGO

Definition of Fraud Risk

Fraud Risk can be defined as follows:

- The risk of intentional or opportunistic acts intended to defraud, misappropriate property or circumvent the law or policies by an internal or external party for expected pecuniary benefit.

- Fraud Risk includes risk associated with system security breaches by internal or external parties where there is an identified intent to gain a pecuniary benefit as classified under Fraud Risk, as opposed to Information Security Risk.

Designing Your Anti–fraud Policy

BANKERS ASSOCIATION OF TRINIDAD AND TOBAGO

Examples of Fraud

- Embezzlement
- Forgery
- Misappropriation of Funds
- Identify Theft
- Online Fraud
- Cyber Related Fraud
- Cheque fraud
- Counterfeit Currency
- Credit/Debit Card Fraud

Designing Your Anti-fraud Policy

Policy and Procedure Development

- Guidance as it relates to anti-fraud activities must continue to be developed and communicated appropriately.
- The anti-fraud policy should flow directly from the organisation's overall approach for management of operational risk, which includes fraud, both internal and external, and outlines the requirements of how fraud will be identified, measured, assessed, reported and mitigated.
- The organisation must develop and implement appropriate guidelines in order to ensure all of their functions are in compliance with the Enterprise Anti-Fraud Policy.

Designing Your Anti-fraud Policy

Documents, Policies, Standards and Other sources of information that compliment the Anti-Fraud Policy:

- Code of Conduct
- Conflict of Interest Policy
- Operational Risk Policy
- Information Security Policy
- Corporate Communication Policy

Designing Your Anti–fraud Policy

Plan – How To Response To Fraud

- reporting suspected fraud
- the investigation process
- liaisons with police and external audit
- initiation of recovery action

Questions