COVID-19 Fraud

Alex Beavan, Head of Fraud Investigation
Western Union Business Solutions

WesternUnion WU | Business Solutions

Agenda

- Emerging fraud scenarios during the pandemic
- Business Email fraud
- Key precaution measures

Corporate fraud

A global risk

Fraud impacting organizations can be both general frauds that target any company, to sector-specific frauds.

Corporate fraud can be any fraud committed against an organization.

The media and FBI has highlighted the growing problem with corporate fraud.

Hong Kong, China and Nigeria are countries where instances of fraud origination are notable.

Over US$26.2billion losses since 2016

Increase of 100% losses since 2018

Source: IC3 – Federal Bureau of Investigation Internet Crime Complaint Center. www.ic3.gov

Western Union
Business Solutions and fraud

Improving the client end-to-end experience is extremely important to everyone at Western Union Business Solutions.

Since 2017, we have embarked on an extensive development of our fraud detection and investigation capabilities, resulting in improving our fraud prevention and controls.

Western Union Business Solutions has a dedicated global fraud investigations team to protect the interests of its clients.

The team is highly skilled and includes accredited financial investigators who have dealt with serious and complex fraud and money laundering investigations, organised crime groups, and terrorism.

The team also has many years of experience in both working at Western Union and working with and for law enforcement and are leaders in compliance and associated fraud training.

COVID-19

Different types of fraud

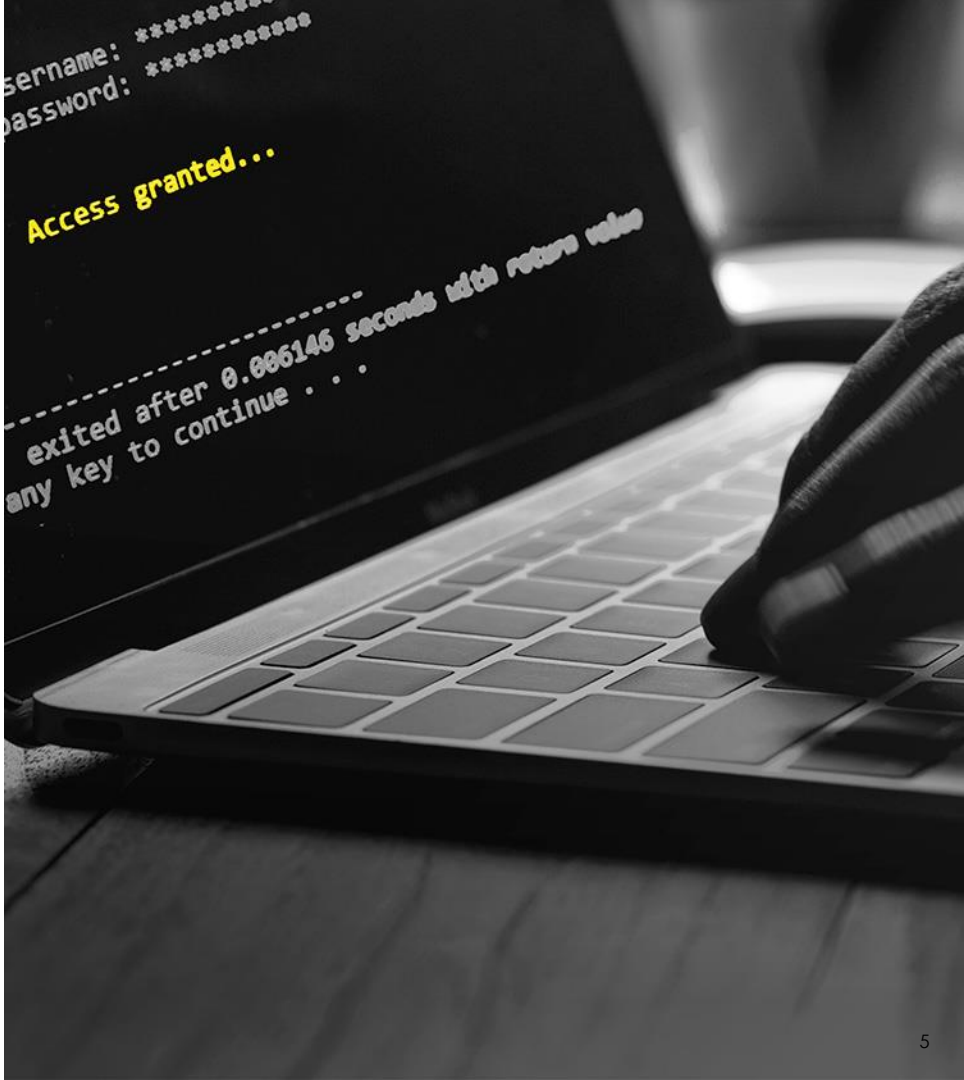
During the ongoing COVID-19 virus outbreak, **fraudsters globally are attempting to exploit the situation** to defraud businesses and individuals.

US citizens have lost more than **USD $100million -** US Federal Trade Commission

Canadian citizens have lost more than **CAD $1.2million -** Canadian Anti-Fraud Centre

---

At Western Union Business Solutions, we feel it is important to alert you to different types of fraud and scenarios that you may be subjected to in the days and months to come, and to inform you of the steps you can take to help prevent you becoming a fraud victim.



Types of Fraud

- Fake goods
- Investment opportunities
- Malicious emails
- Fake charities
- Fake funding

Fake goods

Details

As the demand for resources grows and the pressure on businesses increases it is possible clients will seek new suppliers to meet that demand.

Fraudsters are setting up fake websites and advertising across open source and social media that they can provide, for example goods such as face masks, ventilators, cleaning goods, foods, and domestic sanitary equipment.

The advertising will indicate that supply can be in bulk. It is unlikely to be extremely cheap as fraudsters are aware of the sheer demand for such goods.

Prevention

In order to prevent yourself from being a victim of this type of scam the following steps should be considered:

- **Only deal with a confirmed supplier** either by previous successful purchase, government authorised, or recommended by someone you trust who has had a successful purchase.
- Always **conduct open source searching** around whether there is suggestion that it is a scam.
- Always **use sites such as WHOIS and business registrations** to establish how long the 'new' supplier has been in existence.
- **Use open source** to check out phone numbers and emails provided.

If in doubt, avoid those suppliers

Investment opportunities

Details

The COVID-19 outbreak has affected global markets such as the Dow Jones and FTSE 100. Shares in companies have been deeply affected which is also impacting pensions and dividends. Individuals with liquidity are avoiding financial markets until the perceived 'bottom' has been reached.

Fraudsters are aware of this and have been setting up fake websites and advertising investment opportunities with high returns. They may advertise investment in the Gold market or property and promise substantial returns.

The advertising encourages individuals and companies to make payments to a bank account. Literature via email will be provided and they may provide details relating to alleged registration with local financial regulators.

Prevention

In order to prevent yourself from being a victim of this type of scam the following steps should be considered:

- **Only invest with a financial institution you have previously used successfully**, government authorised, or recommended by someone you trust who has successfully invested.
- Check out the website using WHOIS and business registrations to **establish how long** the investment company has been in existence.
- **Review any alleged financial membership number** with the appropriate website such as the FCA.
- Such opportunities always promise excellent returns which are just not achievable. **Common sense should be used** in any decision making **as to whether to invest.**

Malicious emails

Details

Nearly every piece of news is currently connected with COVID-19. Many Governments and companies are also sending out emails about the virus and how they are dealing with it.

Fraudsters are pretending to be Government organisations / businesses / financial institutions and sending out fake emails designed to trick people into opening attachments that download malicious software.

Such email may have fake screenshots and imagery taken from real and related websites.

Prevention

In order to prevent yourself from being a victim of this type of phishing / malware attacks the following steps should be considered:

- **Never click on any link** or open any attachment within an email unless it's from a known and confirmed contact.
- If you get an email from a website you subscribed to, go directly to the website to check on your account. **Do not use any link in the email you received.**
- **Delete all suspicious emails immediately.** Clear your junk mail regularly as well as your email deletion folder.

Fake charities

Details

The COVID-19 crisis has left a lot of individuals short of supplies and also basic living requirements in certain regions.

Fraudsters are setting up fake websites pretending to be charities and appealing to businesses and individuals for monetary contributions to help individuals and communities affected. The websites have used the copious amount of material out in the public domain to help build their websites to give them an air of authenticity.

The fraudsters are setting up ways to make donations via bank accounts, financial institutions, and fake money services businesses.

Prevention

In order to prevent yourself from being a victim of this type of scam these steps should be considered:

- **Only use a charity or NGO that is properly registered** and has been for a considerable amount of time. Check your regional charities registration website to confirm the authenticity of the charity. Read through accounts, if listed, to help you make an informed decision.
- Always use open source searching to **confirm or deny** whether **an alleged charity** is a suspected scam.

Fake funding

Details

In this scam, clients or individuals receive fake emails, text messages or social media posts asking them to donate money to a research team that is allegedly developing a drug to treat COVID-19. Others claim they are nearing a vaccine for immunizing the public against the virus.

The email will take them to a donation link where they can send a donation to help the advertised cause.

The fraudsters will put imagery and videos in the emails showing people suffering but also provide some technical information apparently linked to the vaccine, as well as videos allegedly to show the vaccine being tested.

Prevention

In order to prevent yourself from being a victim of this type of phishing / malware attacks the following steps should be considered:

- **Never click on any link** or open any attachment within an email not from a known and confirmed contact.
  The same applies to any messages via social media.

- All such projects around **vaccine development** are Government led and **do not involve mailshots asking for donations.**

Do not make any such donations as these are all fake.

Business email fraud

Business email fraud

Business email fraud is a form of fraud where a criminal impersonates an individual known to the victim through a business relationship and attempts to coerce the victim into transferring funds.

Other types of business email fraud include:

Employee account compromise.

Legal/CEO impersonation and fraud.

Compromised account — may be used by fraudsters to steal personally identifiable information.

Fraudsters will also sell compromised account information to other fraudsters to exploit.

Business email fraud

The fraudsters send an email to an individual in the accounting or finance department of a company,

posing as the representative of another company who is currently engaged in business, often concerning an open invoice, requesting a wire transfer.

The request is likely to include a change to previous arrangements

such as a change to the beneficiary name, bank account and location. The fraudsters will often provide reasons for the change in circumstances.

The unsuspecting employee then initiates a fraudulent wire transfer

in the requested amount to the bank account of the fraudster's choosing.

There are 4 stages of business email fraud

Business email fraud can occur in many different forms. However there are four distinctive stages.

Most compromises occur with the client being deceived into altering the beneficiary details. The stages are as follows:

Phishing attempts

Fraudsters who now have access to the business email account.

Impersonation via email

Business receives email from fraudsters impersonating vendor.

Payment redirection

Beneficiary details changed and wire transfer approved.

Payment sent

Fraudsters monitor payment.

Business email fraud - red flags

Change of country for the beneficiary bank

Completely different country from where the customer/supplier has always previously banked.

Changes to the beneficiary name

To either another company name, a personal name **or** a mixture of name and company.

Reason given for change of beneficiary bank

Beware bizarre and illogical business reasons for wanting to get the bank details changes.

Variant or new email address

Variant email address very similar to the correct email address on any email wanting beneficiary changes. Sometimes the email address may even be identical.

Business email fraud - red flags

Inconsistencies in email sent by the fraudsters

Font | Spelling | Grammar | Structure | Time

'New' Invoices not standard of real invoices from suppliers.

Any font changes, poor spelling and/or smaller digital size

Urgency of the alleged "supplier" during email exchanges.

Fraudsters will pressure client to complete transaction quickly with constant emails and social media.

How to protect yourself from business email fraud

Keep records of phone numbers, contact details and email addresses for your vendors

Never just trust the contents of an email

Always confirm verbally beneficiary bank details

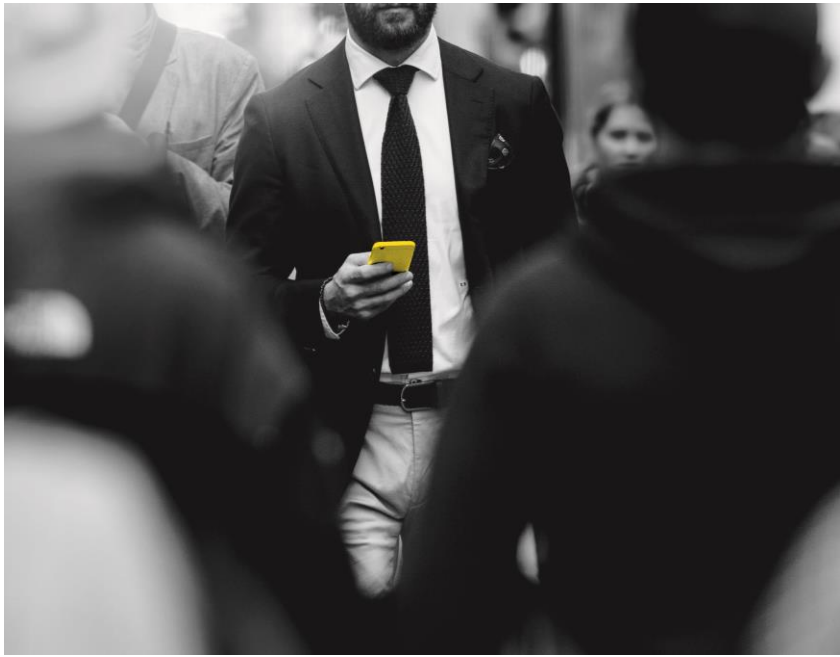
Other steps to take

Consider improved fraud awareness training for your employees and make sure approval processes exist specifically for transactional payments.

Engage with law enforcement when you suspect fraud. Avoiding such issues may do more harm in the long run to the business and reputationally.

As with all business transactions, correct due diligence needs to be undertaken to confirm the veracity of the parties involved. Most important with new suppliers.

Consider a review of your fraud strategy and you prevention/detection program and associated polices. Are your controls adequate?



Alex Beavan
Head of Fraud Investigation
Western Union Business Solutions

Email: alex.beavan@westernunion.com

Western Union Business Solutions is a business unit of The Western Union Company. Services in the US are provided by Western Union Business Solutions (USA), LLC (NMLS ID: 907333; MA MT license #: FT0041) (referred to as "WUBS" or "Western Union Business Solutions"). For a complete listing of US state licensing, visit http://business.westernunion.com/about/notices/. For additional information about Western Union Business Solutions USA, LLC visit http://business.westernunion.com/About/Compliance-Legal.
This presentation does not create any binding obligation on any party, nor does it constitute an offer or a solicitation of an order. Any such offer or solicitation will only be made and the relationship between you and WUBS shall be governed by the applicable terms and conditions and any transaction-specific documentation entered into between you and WUBS. No representations, warranties or conditions of any kind, express or implied, are made herein.
WUBS is the issuer of the products discussed herein and would be a counterparty to any transaction you undertake with us. This presentation is not directed to, or intended for distribution to or use by, any person or entity who is a citizen or resident of or located in any locality, state, country or other jurisdiction where such distribution, publication, availability or use would be contrary to law or regulation or which would subject WUBS or its affiliates to any registration or licensing requirement within such jurisdiction.

WUBS is not registered with the Commodity Futures Trading Commission as a Commodity Trading Advisor, as a Swap Dealer, or in any other capacity. WUBS is not a member of the National Futures Association. Protections that would otherwise be available under the Commodity Exchange Act, the rules of the Commodity Futures Trading Commission, or the rules of the National Futures Association will not be available to you in connection with your relationship with or transactions with WUBS.

Customers may be required to meet certain eligibility requirements in order to enter into foreign exchange transactions with WUBS. Claims regarding the products discussed and other information set out herein are general in nature and do not take into account your specific objectives, financial situation, or needs. This presentation does not constitute financial advice or a financial recommendation. You should use your independent judgment and consult with your own independent advisors in evaluating whether to enter into a transaction with WUBS. WUBS bases recommendations only on general industry knowledge and the client profile you have provided, and WUBS is not undertaking to assess the suitability of any recommendation for your particular hedging needs. WUBS has based the opinions expressed herein on information generally available to the public. WUBS makes no warranty concerning the accuracy of this information and specifically disclaims any liability whatsoever for any loss arising from hedging decisions based on the opinions expressed and information contained herein. Such information and opinions are for general information only and are not intended to present advice with respect to matters reviewed and commented upon.