TEMPUS
Simplifying Global Payments | 20 YEARS

CYBERSECURITY
WE ARE ALL IN THIS TOGETHER

Presented by:

Glenn Kerr, Chief Technology Officer

Michael Lindemann, Chief Compliance Officer

A monex COMPANY

Today's Agenda

- **Current COVID-State of Cyber Threat Landscape**
- **Actual Examples of Thwarted Attacks**
- **How To Cyber-Secure Your Business – Sharing Best Practices**
- **Fraudulent Attacks— Detecting & Mitigating**
- **Mind the Red Flags – COVID-Specific on the rise**
- **Keeping Compliant – Your business and your vendors**

Webinar Logistics

- Approximately 30-minute Zoom webinar is being recorded
- Link to session recording and slides will be sent to attendees within 48 hours

Current State of Cyber Threat Landscape

Being Preemptive Isn't an Option, It's a Necessity

- **WFH Employees aren't thinking about organizational security**
  - Make-shift work environments
  - Balancing on/offline distractions
  - Novice usage of new digital platforms, applications & processes
- **Cyberattacks increasingly focus targeting employees**
  - Phishing attacks remain top tactic
  - Seeking direct access to user credentials, applications & data
  - Employee is usually your last line of defense
- **'Remote workstyle' messaging provides ideal disguise**
  - Familiarity with messages & text 'normalize' scams
  - Use of shipping, billing, and banking stories
  - Impersonating domains, businesses, and people
  - Increased use of WFH tools(Zoom, Teams) provide greater bounty

Phishing Examples

How To Spot Phishing Fraud Attempts

- **Poorly written**
- **'From Email Address' looks suspicious**
- **'From Domain' is slightly misspelled**
- **Suspicious Links in email**
- **Suspicious Attachments**
- **Sense of urgency in message**

Your PayPal Access Blocked !

PayPal <paypalaccounts@mailbox.com> Unsubscribe Feb 17, 2019, 4:50 PM
to me

Your PayPal Account is Limited, Solve in 24 Hours!

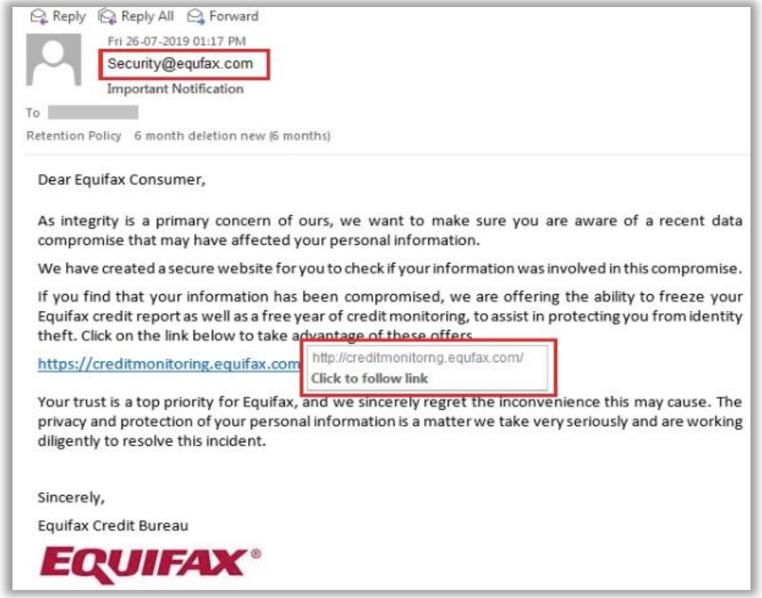
Dear PayPal Customer,

We're sorry to say you cannot access all the paypal account features like payment and money transfer.
Click here to fix your account now..

Why is it blocked?
Because we think your account is in danger of theft and unauthorized uses.

How can I fix the problem?
Confirm all your details on our server. Just click below and follow all of the steps.

Confirm Account Details Now



Reply Reply All Forward

Fri 26-07-2019 01:17 PM
Security@equfax.com
Important Notification
To
Retention Policy 6 month deletion new (6 months)

Dear Equifax Consumer,

As integrity is a primary concern of ours, we want to make sure you are aware of a recent data compromise that may have affected your personal information.

We have created a secure website for you to check if your information was involved in this compromise.

If you find that your information has been compromised, we are offering the ability to freeze your Equifax credit report as well as a free year of credit monitoring, to assist in protecting you from identity theft. Click on the link below to take advantage of these offers.

https://creditmonitoring.equifax.com

http://creditmonitorng.equfax.com/
Click to follow link

Your trust is a top priority for Equifax, and we sincerely regret the inconvenience this may cause. The privacy and protection of your personal information is a matter we take very seriously and are working diligently to resolve this incident.

Sincerely,

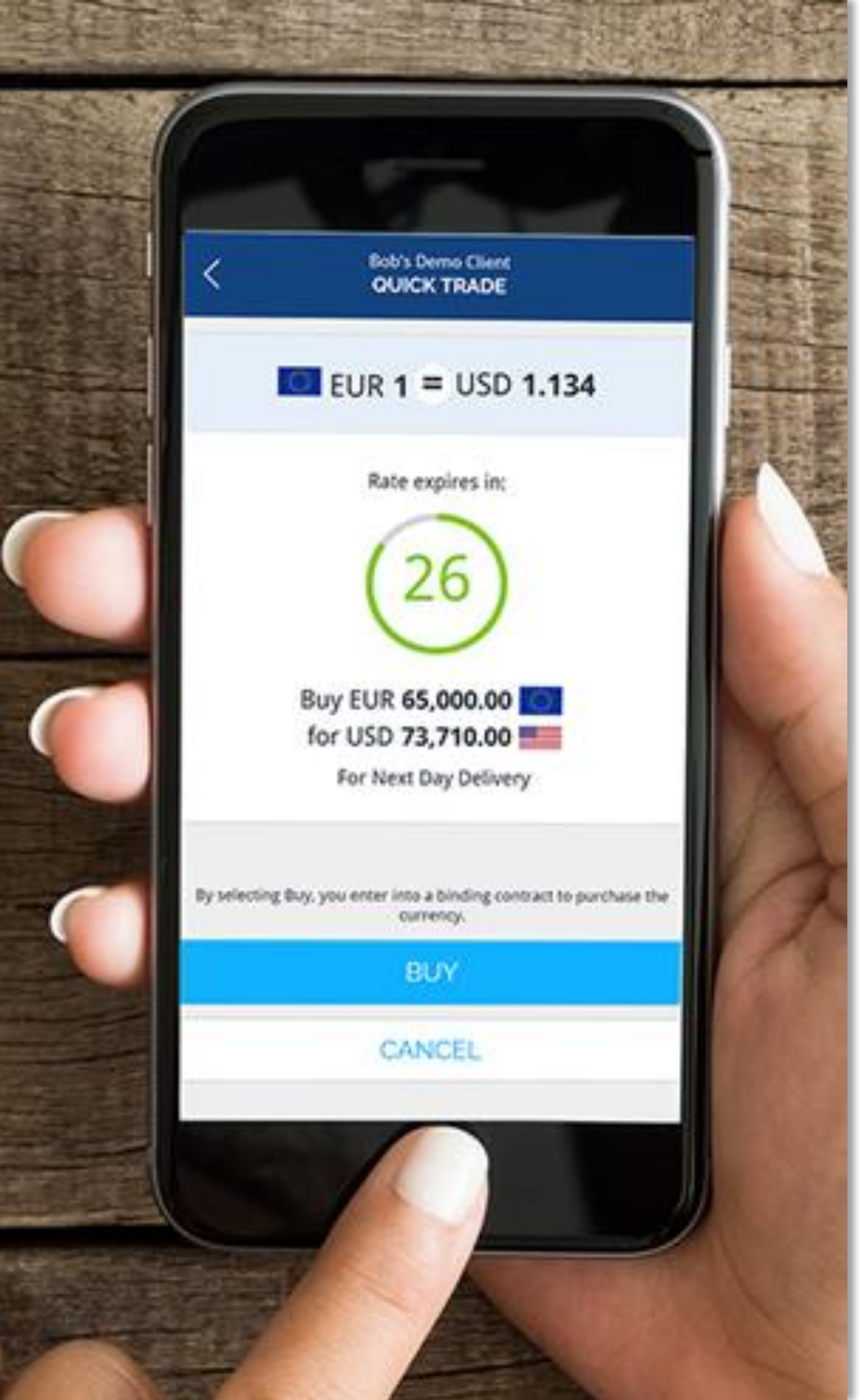
Equifax Credit Bureau

EQUIFAX®

Share Best Practices

Mitigate Through Shared Awareness & Vigilance

- **Two-Factor Authentication (2FA)**
  - Ensure all your accounts, banking & email for example, are 2FA protected
- **Smart(er) Password policies**
  - Use passphrases instead of passwords (but not company-related words)
  - Never reuse passwords cross-accounts, avoid common phrases of personal significance
  - Use strong passwords with mix of alpha, numbers and special characters
- **Internal checks and balances**
  - Don't send wires out without verbal confirmation
  - Any banking (wire or debit) instructions verbally confirmed with requesting party
- **When in doubt, don't click**
  - Never click external email links or attachments unless you are expecting it
  - Phishing attempts increase during crisis
- **Virus Protection**
  - Ensure updated, active subscription with real time scanning
  - Schedule routine, daily scanning



Tempus Online

Options to Secure Your Payments Experience

User Options

- **Two-Factor Authentication** – Sign Up!
- **User activity alerts**
  - Adding beneficiary
  - Editing Beneficiary
  - Password change
  - User locked out
  - Login from unfamiliar device

System Settings

- **Special password requirements**
  - Complexity
  - Lockout after 3 attempts
- **Captcha**
- **Alerts**
  - Suspicious country logins

Fraudulent Attacks

Detecting and Mitigating

MITIGATION

- **Verify claims through a known contact**—do not reach out through provided information
- If immediate delivery is impossible, route payments to a holding or escrow **account**
- Verify with the manufacturer or verified distributor that the **seller is legitimate**
- **Be skeptical of last-minute changes** in wiring instructions or recipient account information
- **Verify email address** used to send emails, especially when using a handheld device.

DETECTION

- **Pre-payment options substantially increases risk** of a buyer being defrauded
- **Donation themed scams** urging recipients to consider donating to WHO
- **Scarcity of certain products** (i.e., PPE) has influenced illicit actors on the market to exploit the global pandemic
- **New company formed** in order to fraudulently apply for government support

Mind the Red Flags

COVID-specific On the Rise

- The seller or broker is **not an entity with which the buyer has an existing business relationship**, or the buyer's existing business relationships are a matter of public record
- **The seller or broker cannot clearly explain** the origin of the items or how they are available given current demand.
- The **potential buyer cannot verify** with the product manufacturer that the seller is a legitimate distributor or vendor of the product, or otherwise verify the supply chain is legitimate.
- **Unexplained urgency** to transfer funds or a last-minute change in previously-established wiring instructions.

COV19 Scams

Recent Developments

- Criminals are **targeting sectors badly affected by the crisis** to launder money and mix funds that are normally laundered via other entities.
- **Unsolicited healthcare or FMLA fraud schemes** of testing and treatment through emails, phone calls, or in person contact.
- **Blackmail attempts**, work from home **scams**, paying for non-existent treatments or equipment, or investment scams.
- **Unsolicited** telephone calls and e-mails from individuals claiming to be **IRS and Treasury employees**. Remember IRS's first form of communication is by mail - not by phone.
- **Sales of counterfeit, tampered, or otherwise fraudulent PPE**, including N95 masks, gloves, and surgical gowns.

Keeping Compliant

Protecting Your Business and Your Vendors

- **Know Your Customer ("KYC")**
  - No longer a tacit reporting requirement; now a key responsibility
  - Utilize resources to validate detailed information, free & paid
- **Utilize digital technologies**
  - Supplement manual support as financial crime increases and becomes more difficult for financial institutions
  - Google: ~launder OR ~laundered OR ~laundering OR ~fraud
- **Enhance Business Continuity Plan (BCPs)**
  - Tailor to new environment, adjusting policies, procedures, and controls
- **Verify relationships with customers' vendors**
  - Time spent on the front-end reaps rewards
  - Fully understand source of funds/income opportunities
- **Pandemic-affected Industry Sectors**
  - Sectors, negatively or positively, affected by the crisis require greater scrutiny
  - Opportunity for criminals to launder funds over high-risk products

Thank You For Joining Us

800.834.2497 | TempusFX.com

Glenn Kerr
Chief Technology Officer
it@tempusfx.com

Michael Lindemann
Chief Compliance Officer
compliance@tempusfx.com