Building Success. Together.

10 Best Practices to Prevent Wire Fraud

Tips to implement now to protect you and your customers.

American Bankers Association®

The following presentation is for information and discussion purposes only. Any views or opinions expressed are the speakers'; shall not be construed as legal advice; and do not necessarily reflect any corporate position, opinion or view of ABA Insurance Services Inc., or its affiliates, or a corporate endorsement, position or preference with respect to any contractual terms and provisions or any related issues. If you have any questions or issues of a specific nature, you should consult appropriate legal or regulatory counsel to review the specific circumstances involved.

The information presented is intended to provide guidance and is not intended as a legal interpretation of any federal, state or local laws, rules or regulations applicable to your business. The loss prevention information provided is intended only to assist policyholders in the management of potential loss producing conditions involving their premises and/or operations based on generally accepted safe practices. In providing such information, ABA Insurance Services Inc. does not warrant that all potential hazards or conditions have been evaluated or can be controlled. It is not intended as an offer to write insurance for such conditions or exposures. The liability of ABA Insurance Services Inc. and its affiliated insurers is limited to the terms, limits and conditions of the insurance policies underwritten by any of them.

© 2019 ABA Insurance Services Inc. dba Cabins Insurance Services in CA, ABA Insurance Services of Kentucky in KY and ABA Insurance Agency Inc. in MI. 3401 Tuttle Rd., Suite 300, Shaker Heights, OH 44122.

Overview

PART 1

- Insurance claims statistics and FBI crime data show wire fraud crime results in higher dollar losses than any other type of cyber crime.

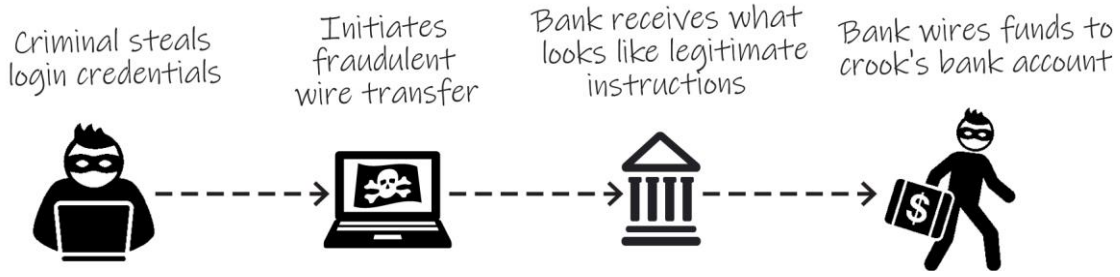
PART 2

- Techniques are available to help you prevent wire fraud.

What is Wire Fraud?

From a bank's perspective, wire fraud is the crime of a fraudulent wire instruction.

Someone pretending to be your customer tricks you into wiring money out of that customer's account.



American Bankers Association®

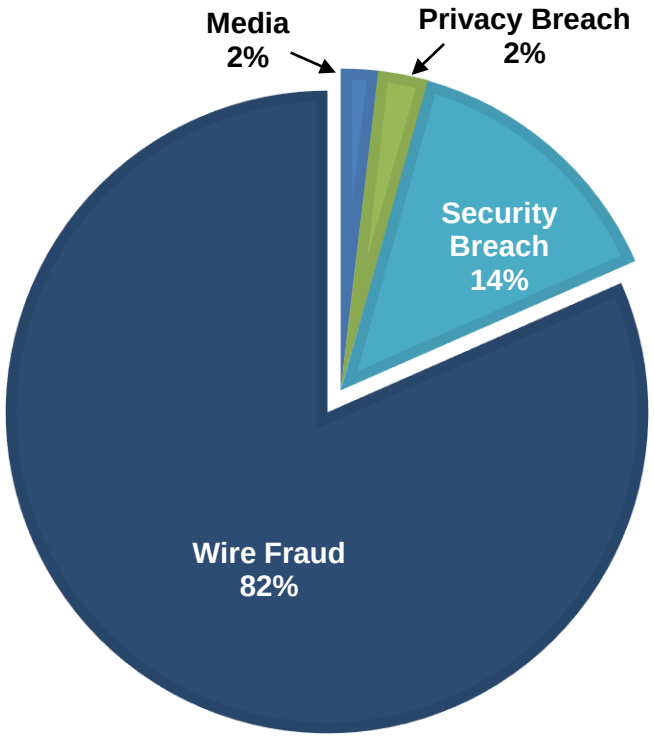
Poll Question

Has your organization ever experienced a wire fraud?

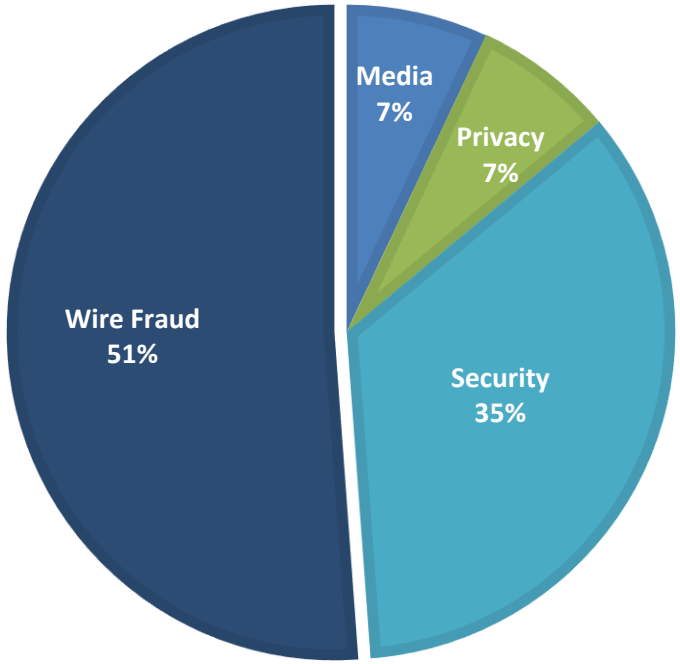
American Bankers Association®

Cyber Claims by Claims Type

ABA Insurance Services Claims Data
Inception-to-Date Dollar Losses



ABA Insurance Services Claims Data
Inception-to-Date Paid Claims Counts

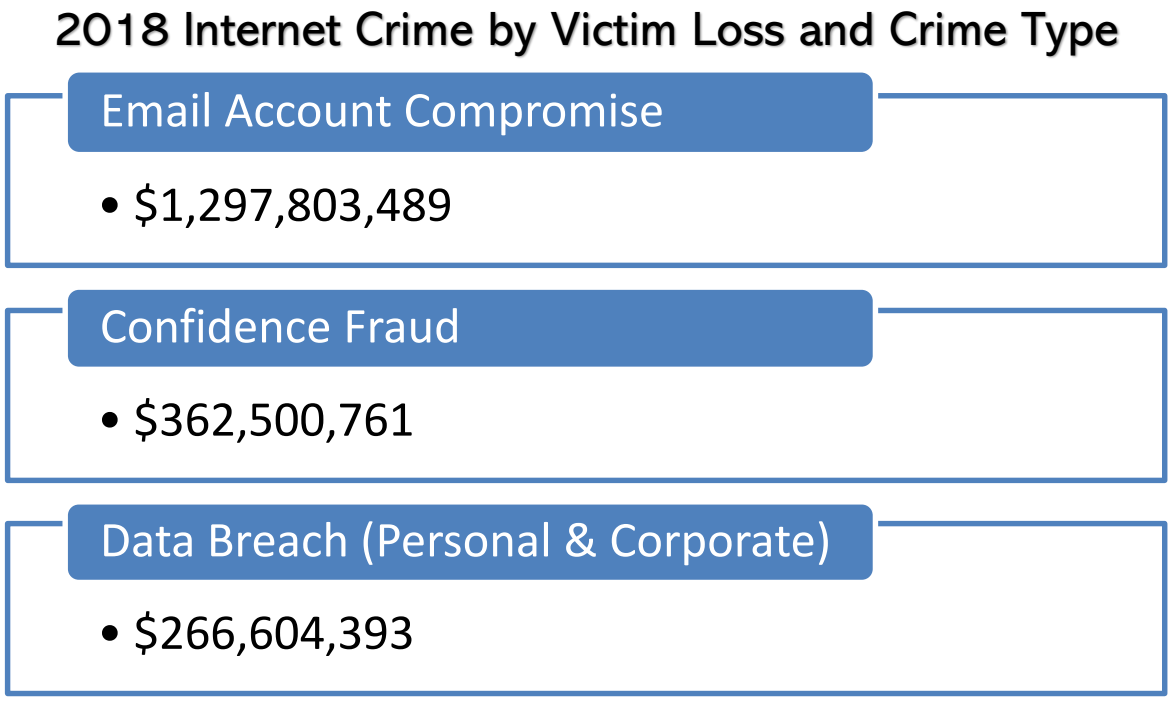


Program insureds have lost more than $50 million in wire fraud scams.

American Bankers Association

What you (probably) already know

Loss from Email Account Compromise, a scam involving compromised email accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds, dwarfs all other Internet-based crimes.

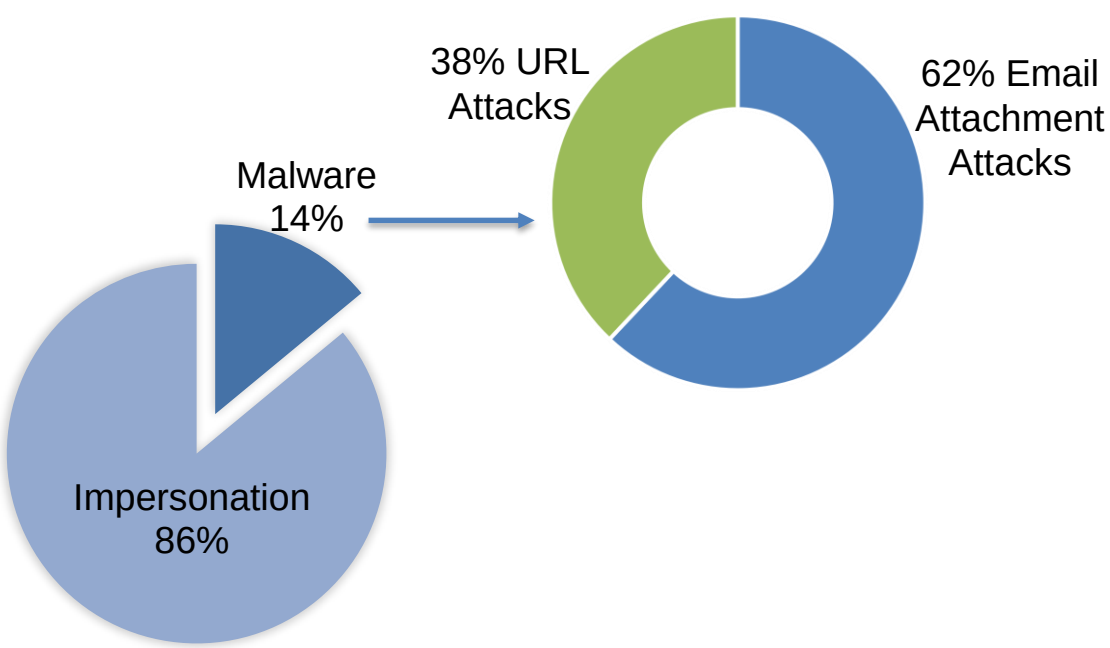


https://www.fbi.gov/news/stories/ic3-releases-2018-internet-crime-report-042219

Email Account Compromise

91% of cyber attacks start with an email

Email Compromise by Source



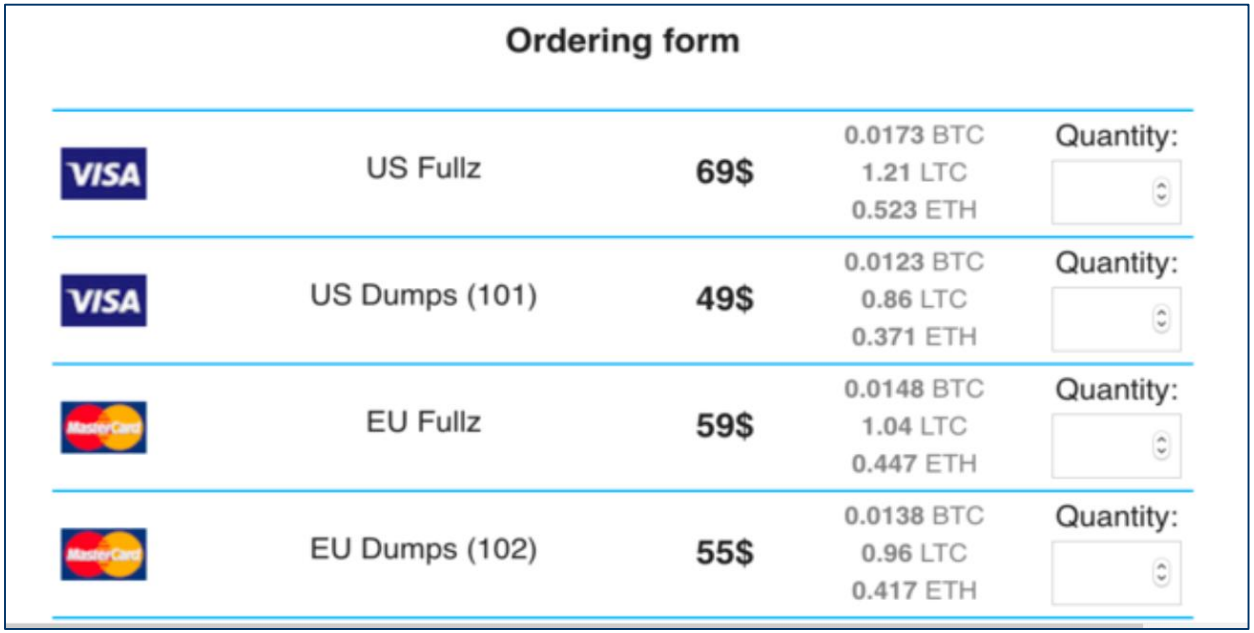
Higher Frequency on Thursdays, Fridays and End of Month

Source: FireEye's The 3Ts of an Email Attack

American Bankers Association

Data Breaches and the Dark Web

Dark web markets sell narcotics, weapons, forged documents and stolen bank credentials.



Ordering form

VISA	US Fullz	69$	0.0173 BTC 1.21 LTC 0.523 ETH	Quantity:
VISA	US Dumps (101)	49$	0.0123 BTC 0.86 LTC 0.371 ETH	Quantity:
MasterCard	EU Fullz	59$	0.0148 BTC 1.04 LTC 0.447 ETH	Quantity:
MasterCard	EU Dumps (102)	55$	0.0138 BTC 0.96 LTC 0.417 ETH	Quantity:

Insurance Notes

Coverage may be triggered under the Financial Institution Bond or a Management or Cyber Liability Policy.

Bond

- Funds Transfer Fraud
- Direct Loss
- Written Agreement
- Verifications

Liability

- Errors & Omissions
- Wrongful Act
- Customer Demand

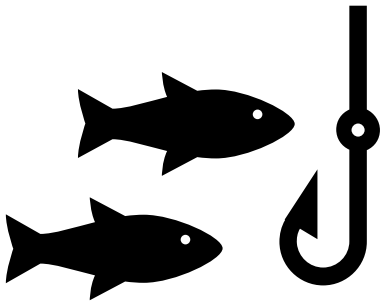
American Bankers Association®

The 10 Best Practices

1. Train Employees
2. Educate Customers about the Risks of Being Phished
3. Use Written Agreements
4. Perform Callbacks (or)
5. Perform Out-of-Band Verifications
6. Pay Special Attention to International Wires
7. Pay Special Attention to HELOCs (and any LOCs)
8. Pay Special Attention to Real Estate Transactions
9. Do Not Immediately Refund Lost Funds to the Customer
10. Do Immediately Recall Lost Funds from the Corresponding Financial Institution

1. Train Employees (Part 1)

To Identify Phishing Emails



What is it?

Criminals attempt to “phish,” or catch employees into opening tainted emails with bad URLS or attachments, which allows the criminals to infiltrate an employee’s computer and potentially, the bank’s network**.**

What can happen?

- Criminals can pose as the employee
- Criminals can access bank or customer information and use it to perpetrate a wire fraud.

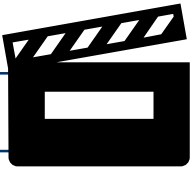
1. Train Employees (Part 1)

To Identify Phishing Emails (continued)

Communicate to Your Employees:

- Email addresses can be spoofed.
- Subject lines often include enticing or threatening language.
- Hover over links before clicking to examine URL.
  - Beware of alternate domain names (not .com or .org).
  - Beware of shortened URL names (tinyurl).
- Beware of clicking on attachments (DocuSign lures highest hit rate).
- Phishers use real company images and real employee names.
- Any phishing attempt—successful or not—should be reported to IT.

DO: Train annually and spot test employees.

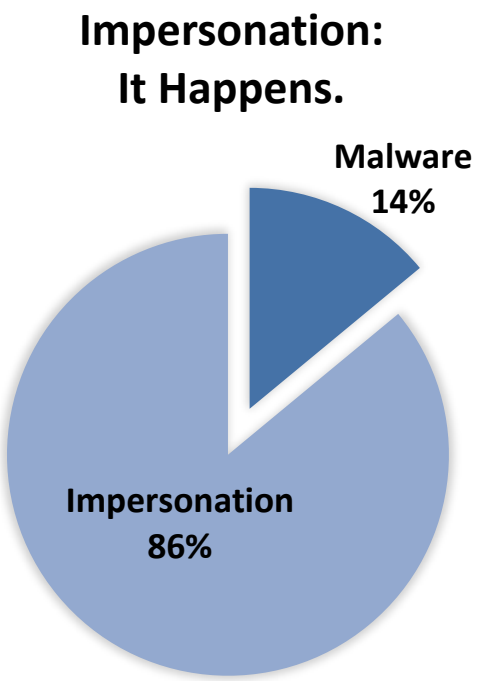


1. Train Employees (Part 2)

To Understand the Risk of Wire Fraud Impersonation

- The average successful email compromise attack earns the cyber criminal $130,000.
- The FBI reported there were over $1 billion in losses resulting from email compromise frauds in 2018 (from over 20,000 attacks).
- Wire Fraud usually has to run through a bank.
- Electronic cash is still cash.

Source: FBI's 2018 Internet Crime Report, pdf.ic3.gov/2018_IC3Report.pdf



Source: FireEye's The 3Ts of an Email Attack

American Bankers Association

1. Train Employees (Part 2)

To Understand the Risk of Wire Fraud Impersonation (continued)

Be on the lookout for these wire fraud instruction red flags:

- It's a rush request.
- Sender insists on solely using email communications.
- Instruction contains odd phrases or misspellings.
- Current request is inconsistent with previous transfers (size or new location).
- We are going into a long weekend.

Fraud increases on Friday

American Bankers Association®

2. Educate Customers About the Risk of Being Phished

Almost 50% of email compromise attacks ultimately seek to initiate a wire fraud. If your customers get phished, there is a good chance that a related wire fraud will be run through your bank. Avoid a potential conflict with your customers and seek to educate them on threats to their hard-earned money from phishing attempts and other cyber crimes.

Resources:

ABA

FTC

From October 8th, 2019 ABA Newsbytes

Survey: Customers Want Cyber Education from Banks

More than 9 in 10 Americans are concerned about their security online, and 74% of consumers say they would be likely to participate in a cybersecurity education or awareness program if their bank offered it, according to a new survey conducted for bank technology firm CSI.

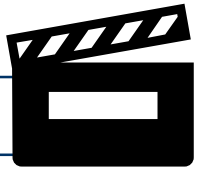
3. Ensure That You Have Written Agreements with Customers In Place

A written agreement is a document that outlines your customer's preferences regarding the transfer of funds from a particular account. You should have a written agreement in place prior to the first wire transfer request.

The agreement should:

- Include the customer's explicit authorization for the bank to execute wires, and the means by which wire transfer requests may be requested (e.g., via email, telephone, or in person)
- Contain the names of all individuals granted authority by the customer to initiate such requests
- Outline a commercially reasonable security procedure that will be utilized by the bank and the customer to authenticate all requests.

DO: Have a Written Agreement with customers prior to wiring funds.



3. Ensure That You Have Written Agreements with Customers In Place, continued

Please note:

- A wire request—a form completed by the customer to initiate a specific wire transfer—**is not the same as a written agreement.**
- The absence of a written agreement will likely result in a claim denial with many insurance carriers.

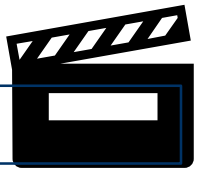
Poll Question

Does your organization require Written Agreements?

4. Perform a Callback on Wires to a Predetermined Phone Number

- A phone call to the customer's number ***on file*** is one of the best ways to prevent wire fraud. This helps to circumvent emails that have been compromised.
- Fraudsters often seek to change the phone number on file, so be wary of any recent change requests. Legitimate changes to established wiring authorization instructions are rare–***assume fraud if recent account changes on file have been made and seek independent verification.***

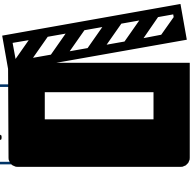
DO: Perform a callback, especially for requests involving large sums.



5. Perform an Out-of-Band Verification

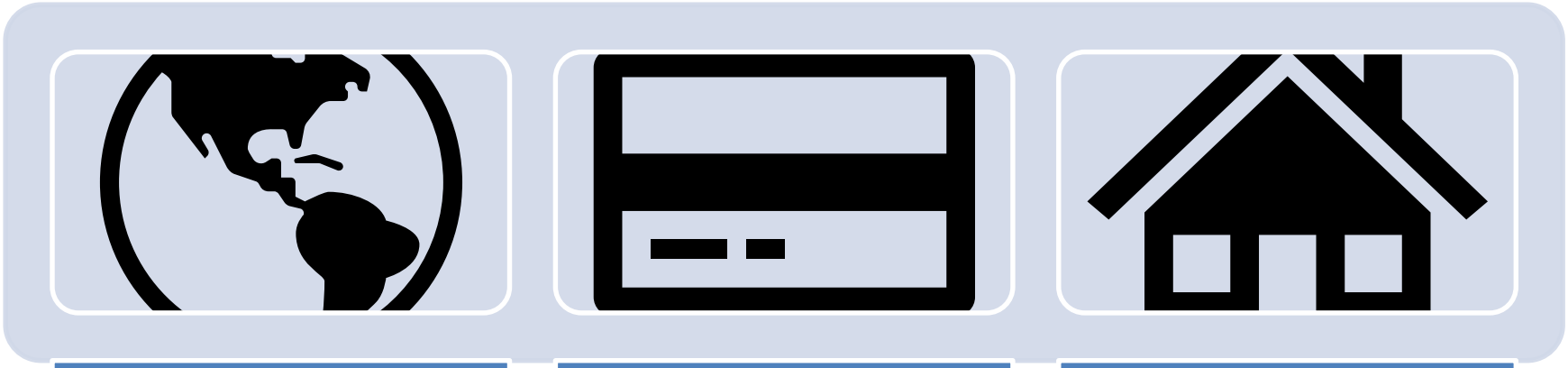
- When a callback is not practical or preferred by the customer, use an out-of-band verification to authenticate wire requests.
- *The type of verification method should be established in the written agreement.* Do not sacrifice sound authentication procedures for customer convenience.

Out-of-Band verification is a process whereby the authentication of a wire request requires two different confirmations from two different channels. Out-of-Band verification will block many types of fraudulent impersonation.



DO: Perform an Out-of-Band verification as outlined in the Written Agreement.

6, 7 and 8. Require extra scrutiny of:



International Wires	Disbursements from HELOCs and other Lines of Credit	Real Estate Transactions

American Bankers Association®

9. Do Not Immediately Refund Lost Funds

While business decisions to immediately restore stolen customer funds are good for the customer relationship, such business decisions are not insurable.

Contact your insurance carrier to report the fraud first and work with the carrier to lay out the best course of action.

Be aware that coverage under a liability policy requires:

- A written demand from the customer requesting the restoration of funds or alleging a wrongful act;
- Legal liability on the bank's part; and
- The Insurer's consent before any settlement with the customer can be made.

10. **DO** immediately attempt to recall lost funds from the corresponding financial institution.

Maximize your chances of retrieving stolen funds:

1. Initiate a SWIFT recall.
2. Contact the fraud department of the receiving bank so they can freeze the funds in the recipient's account.
3. If the funds have already moved, ask the recipient bank to find out where the money was sent and ask them to contact the third bank to freeze the funds in that account.
4. Contact the customer and encourage them to loop in their IT team.
5. Contact (or have the customer contact) the FBI's Internet Crime Complaint Center.

Timeliness is Key!

When stolen funds arrive in the fraudster's bank account, a network of money launderers is immediately engaged to withdraw the stolen cash or rewire the money to subaccounts. This is called "Money Muling."

We welcome your questions at this time.

Thanks for your participation

ABA Insurance Services' Contact information

Lisa Micciche, Senior Product Manager
lmicciche@abais.com
216-220-1297

Ann Gardiner, Bond Claims Manager
agardiner@abais.com
216-220-1305

American Bankers Association