When minutes matter

A step-by-step guide to wire fraud recovery

Created and published by:

Thomas W. Cronkright II, Esq.
CEO/Co-Founder
CertifID LLC
1410 Plainfield Ave. NE
Grand Rapids, MI 49505
616.855.0855
www.certifid.com
tcronkright@certifid.com

Kenneth S. Robb, CISSP
Cyber Security & Risk Consultant
Citadel Cyber Solutions, Inc.
322 North Shore Dr. BLDG 18, Suite 200
Pittsburgh PA 15212
412-203-2207
www.citadelcybersolutions.com
ken.robb@citadelcybersolutions.com

Updated: May 18, 2018
Wire fraud is rapidly becoming an epidemic in the mortgage industry. The FBI (IC3) hit a milestone last year by receiving its four-millionth complaint since the IC3 division was created in 2000. In 2017, it received 301,580 cybercrime and fraud complaints with reported losses over $1.4 Billion - Business Email Compromise (BEC) was the No. 1 cause of loss and is now being tracked as a separate cybercrime.

The number of BEC victims increased 31% from 2016 to 2017 and BEC-related losses during the same period increased by 88%. Astonishingly, that number is estimated to include just 15% of the actual number of wire fraud incidents to hit the industry (Source: IC3). A tidal wave of indicators and anecdotes leave little doubt that fraudsters are only growing more sophisticated, more aggressive and more successful each day.

What follows is our suggested roadmap for those businesses—and not simply title insurance-related firms, but any mortgage-related businesses—that believe they've been victimized by a wire fraud scheme. It cannot be overstated: if you believe you or your firm has been touched by mortgage fraud, there is no margin for error and no time to waste. If you hope to make any recovery of the stolen funds whatsoever, minutes matter, and your course must be unwavering.

Although we cannot guarantee that simply following our roadmap will invariably bring about a full recovery of any misappropriated funds, we can say with certainty that it is the path which best maximizes any chance of recovery you do have. We are also sharing this information because we believe not enough businesses and thought leaders in the housing and mortgage industry have fully accepted the very real and very widespread nature of the wire fraud threat. Awareness and preparation are the natural predators of any type of fraud. Please consider what follows to be not only a roadmap to recovery, but a wake-up call to the nature of the threat itself.

Don’t just be a squeaky wheel. Be a tornado siren. When you are a victim of wire fraud, you must immediately become your own advocate for recovery. In that process, you will undoubtedly encounter inertia, skepticism and other forces that will only delay (or prevent) recovery. You must be aggressive, persistent and determined to complete the steps necessary to confirm the activity of all third parties you have engaged. This is much more than a “squeaky wheel” moment. You must be the tornado siren that people cannot and will not ignore, and you must stay in that mode until you’ve received the information and confirmations you need in order to make a recovery.

Tick-Tock. Time is not your friend. From the moment you learn of a wire fraud, the best chance of recovery is to follow the steps outlined below. Time is of the essence. The ability to recover funds decreases exponentially as more time lapses between the discovery of the event and your actions. This process is going to be a frantic series of events; however, if you plan properly you increase the odds of recovering your funds and mitigating further loss.

Finally, we’ve included helpful law enforcement contact information (Exhibit A) and sample court pleadings (Exhibit B) should you find yourself the victim of wire fraud. We also welcome your feedback.

If you have suggestions, anecdotes of your own or questions, please visit us at www.citadelcybersolutions.com and www.certifid.com.
Step 1: Contact your bank and have a “fraud alert” sent to the bank that received your wire.

- Call your bank and notify them of the fraudulent wire;
- Include all information on the wire transfer that was sent (including any reference numbers from the Federal Reserve);
- Demand that they immediately contact the fraud department of the receiving bank and place a “fraud freeze” on the account so your money cannot be further transferred; and
- Demand that they confirm whether your funds are still in that account and, if not, (i) identify where the funds were subsequently transferred; and (ii) immediately notify any banks that received your funds to place a “fraud freeze” on those accounts.

Step 2: File a complaint with the FBI’s Internet Crime Complaint Center (IC3).

- Go to https://www.ic3.gov/complaint/default.aspx/ to file a complaint with IC3 (www.IC3.com) and be prepared to provide the following information:
  - Victim’s name, address, telephone, and email;
  - Financial transaction information (e.g., account information, transaction date and amount, who received the money);
  - Under the Financial Transaction(s) section of the form, select “Wire Transfer” from the Transaction Type drop down menu.
  - Subject’s name, address, telephone, email, website, and IP address;
  - Specific details on how you were victimized;
  - Email header(s); and
  - Any other relevant information you believe is necessary to support your complaint.
- Note and retain your IC3 Complaint Number – you will need to give that to the FBI field office (see below).

NOTE: FILING A COMPLAINT WITH THE FBI IS NECESSARY BUT DOES NOT ENGAGE A REAL-TIME RECOVERY EFFORT. YOU MUST COMPLETE THE REMAINING STEPS TO INCREASE YOUR CHANCE OF RECOVERY.
Step 3: Contact your local FBI field office and provide the IC3 complaint number.

- Go to: https://www.fbi.gov/contact-us/field-offices and find the field office nearest you – please see Exhibit A for a full contact list of FBI field offices by state and county;
- Call the field office and ask for a special agent that processes financial or cyber crimes;
- Give the special agent the IC3 complaint number, explain the facts leading up to the wire transfer and share any other critical information; and
- Share your contact information with the special agent so they may get back in touch with you.

Step 3.1: (For Enterprise Frauds): Contact legal counsel to determine if an injunctive order is necessary.

- If required, contact legal counsel to file pleadings and request an injunctive order (commonly referred to as a “temporary restraining order”) naming all banks that received your funds and preventing them from any further transfer of funds from such accounts. Please see Exhibit B for an example of such pleadings, motions and orders; and
- Serve the injunctive order on the bank(s) and confirm receipt by the bank(s).
Step 4: Contact all banks that may have also received your funds.

- Call the bank where the money was initially wired and ask to speak to someone in its fraud prevention group;
- Provide all information about the wire transfer so the bank can accurately identify the transfer and the account;
- Request that the bank initiate a “fraud freeze” on any further transfers from the account that received your funds;
- Confirm that the “fraud freeze” is in place and determine how long it will remain in place;
- Ask if any funds have been wired from the account since your funds were deposited. If so, (i) ask for the names and locations of the bank(s) that received your funds; and (ii) request the bank to send a message to the bank(s) requesting a “fraud freeze” on those accounts; and
- Write down the number you used to contact the bank, the time of the call, and the name of the bank representative you spoke with. Be sure to obtain a direct call back number and the email address of that representative for future correspondence.

NOTE: IF MORE THAN ONE BANK RECEIVED YOUR FUNDS, REPEAT STEP 4 FOR ALL OTHER BANKS.

Step 4.1: (For Enterprise Frauds): Contact your insurance carrier.

- If you hold errors and omissions coverage, professional liability coverage or any form of cyber security or cyber loss coverage, contact your insurance agent and place your insurer on notice of the incident.

Step 5: Contact local authorities and file a police report.

- Call the local authorities and file a police report;
- Provide local authorities with all relevant information;
- Save the incident number or police report number for further reference; and
- Share all contact information with the local authorities for future communication.
Step 6: (For Enterprise Frauds): Contact your security team, IT department or consultant and initiate “The Information Technology Kill Chain”.

- If you have an incident response plan in place your IT/Security team may have already started the process of responding to the incident. If you do not have an incident response plan in place you need to follow the basics step outlined below in response to the compromise.

- Determine the source of the breach.
  - Most wire fraud attacks result from simple Business Email Compromise (BEC): An attacker has gained access to your email system through some means (phishing email, social engineering, or brute force). If your email is hosted onsite it could be a deeper penetration of the network and more serious intrusion; and
  - In more serious cases, the attacker may have installed malware on your machine and/or network that has not only compromised your email credentials but your credentials to other key company and personal systems. This is a more serious issue and needs to be dealt with swiftly and immediately.

- Contact your internal or external security/IT group before changing any settings or configurations on the environment;

- Contact your internal or external security/IT group to explain the situation and that a full “image” of the system needs to be created for eForensic purposes;
  - If possible, use a clean loaner system to conduct business using a different temporary email address.

- If warranted, eForensics investigators can be dispatched from a variety of sources to investigate the incident to determine if the data suggests greater impact on the environment.
Details should come quickly, but the money may come back slowly.

If everyone is engaged in the recovery effort, you should have a good understanding of where your money is and the likelihood of recovery. You must keep the pressure on until you get answers to those questions.

The actual return of your funds may take significant time depending on the institution and circumstances.

Be prepared to “indemnify” the bank returning the funds.

Most banks will require you to sign an indemnity agreement before they will return funds to you. Have legal counsel standing by to review and return the indemnity agreement.

The indemnity agreement will come from the bank returning the money, not the bank you used to send the money in the first place.

Don’t trust anyone proactively reaching out to you about your fraud.

If you receive a call from someone identifying herself as being with a bank, the FBI or any other entity she claims is aware of your circumstances and working toward your recovery – DO NOT TRUST THAT CLAIM. Verify and double-check the authenticity of her identity.

Cyber criminals know when money is sent. One of their tactics, to create more time to move the money overseas, is to call or email the person being defrauded and pose as a bank or FBI representative working to recover the funds. You cannot trust any inbound communication without independently verifying the person’s identity and credentials on your own. It is likely a fraudster trying to put someone’s mind at ease while taking advantage of precious recovery time.
Planning and preparing for the next incident

**Preparation**
1. Create and review incident response policies as well as conducting a thorough risk analysis of your environment.
2. Train! Simulate incidents and test response activities. Confirm compliance with policies;
3. Post policies in key departments.
4. Engage third parties to review and update policies to ensure best-practice responses; and
5. As a starting point, see our Data Security and Best Practices Guide at: Exhibit C

**Detection**
6. The timing of detection is critical. You typically have 48 hours or less to recover funds.

**Response**
7. Containment is critical once the event is discovered and further damage must be mitigated.
8. No changes should be made on the device or devices impacted without security/IT approval.
9. An image of the system(s) should be executed and stored for forensic investigators.

**Mitigate**
10. Build an understanding of what was compromised on the system, so the system can be properly recovered.
11. The method of recovery will be dependent on this phase and remediation steps will begin here.

**Report**
12. This should not be confused with the above-mentioned reporting of the “Financial Fraud Kill Chain”. This is information that should be collected and used for informing key stakeholders as well as future training to demonstrate the incident as part of the preparation phase noted above.

**Recover**
13. In connection with the mitigation efforts, remediation could be a simple email password change or as involved as rebuilding the machine. At this point, the system is restored to its former operational status.

**Post Mortem**
14. Obtain and document a comprehensive summary of the events that lead to the breach or loss.
15. New risk mitigation controls should be implemented to prevent further incidents - once we know better, we should do better.

CertifiD is a guaranteed solution that prevents fraud and restores trust in transactions. Harnessing and analyzing billions of combined personal, and digital records, a “digital truth” is established that confirms you are exchanging information with the person you intend to. This allows you to act with confidence and focus on the customer experience rather than worrying about fraud.

For more information, or to start a conversation, please visit www.citadelcybersolutions.com and www.certifid.com.
About the authors

**Thomas W. Cronkright II**
Co-Founder and CEO, CertifID

Tom is the co-founder and CEO of CertifID, a real-time and guaranteed identity and document verification system to prevent wire fraud. He and his business partner, Lawrence Duthler, created the solution in response to a fraud incident they experienced in 2015 and the accelerating instances of fraud in real estate transactions. Tom is a licensed attorney, and frequent speaker on identity, cyber fraud, and real estate topics.

Tom is also the co-founder and CEO of Sun Title, a commercial and residential title agent that has been recognized as an Inc. 5000 company for four consecutive years.

Prior to becoming an entrepreneur, Tom was an attorney with two prestigious law firms in the midwest. Tom received his B.A. degree in finance from Western Michigan University and his law degree from Wayne State University.

**Kenneth S. Robb Jr.**
Founder and Senior Advisor, Citadel Cyber Solutions

Ken is the founder and a senior advisor at Citadel Cyber Solutions. With 25 years’ experience in building and managing financial services information technology systems including compliance, workflow, regulatory, and operations management solutions, Ken brings a unique focus to Cyber Security solutions.

Ken serves as the Pittsburgh InfraGard Financial Services IMA Sector Chief, was a 2016 Pittsburgh CISO/CIO of the Year Finalist, serves as an Everwise Senior Technology Mentor, and holds the CISSP certification (Certified Information Systems Security Professional). Ken holds a B.S. in Business Administration from the University of Dayton and an M.S. in Economics from Indiana State University.
Exhibit A

FBI contact information by jurisdiction
### FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alabama</td>
<td>Lauderdale, Limestone, Madison Jackson, colbert, Lawrence, Morgan, Marshall, Dekalb, Marion, Winston, Cullman, Blount, Etoway, Cherokee, Lamar, Payette, Walker, Jefferson, St. Clair, Calhoun, Cleburne, Pickens, Tuscaloosa, Shelby, Talledega, Clay, Sumter, Green, and Bibb Counties.</td>
<td>Birmingham Field Office</td>
<td>1000 18th Street North, Birmingham, AL 35203</td>
<td>(205) 326-6166</td>
</tr>
<tr>
<td>Alaska</td>
<td>all counties</td>
<td>Anchorage Field Office</td>
<td>101 East Sixth Avenue Anchorage, AK 99501</td>
<td>(907) 276-4441</td>
</tr>
<tr>
<td>Arizona</td>
<td>all counties</td>
<td>Phoenix Field Office</td>
<td>21711 N. 7th Street, Phoenix, AZ 85024</td>
<td>(623) 466-1999</td>
</tr>
<tr>
<td>Arkansas</td>
<td>all counties</td>
<td>Little Rock Field Office</td>
<td>24 Shackleford West Boulevard, Little Rock, AR 72211-3755</td>
<td>(501) 221-9100</td>
</tr>
<tr>
<td>California</td>
<td>San Luis Obispo, Santa Barbara, Ventura, Los Angeles, San Bernardino, Orange, and Riverside.</td>
<td>Los Angeles Field Office</td>
<td>11000 Wilshire Boulevard, Suite 1700, Los Angeles, CA 90024</td>
<td>(310) 477-6565</td>
</tr>
<tr>
<td>California</td>
<td>El Dorado, Placer, Sacramento, and Yolo, Inyo and Kern, Butte, Colusa, Glenn, Nevada (western portion) Plumas, Sierra, Sutter, and Yuba, Solano, Fresno, Kings, Madera, Mariposa, Merced, and Tulare, Lassen, Modoc, Shasta, Siskiyou, Tehama, and Trinity, Alpine, El Dorado (mountainous portions), Mono, Nevada (mountainous portions), and Placer (mountainous portions), Amador, Calaveras, San Joaquin, Stanislaus, and Tuolumne</td>
<td>Sacramento Field Office</td>
<td>2001 Freedom Way, Roseville, CA 95678</td>
<td>(916) 746-7000</td>
</tr>
<tr>
<td>California</td>
<td>San Diego, Imperial, San Diego County (area north of Del Mar, east to Borrego Springs), including the following incorporated and unincorporated cities: Bonsall, Borrego Springs, Camp Pendleton, Cardiff, Carlsbad, Del Mar (incorporated city only), Encinitas, Escondido, Fairbanks Ranch, Fallbrook, Leucadia, Oceanside, Olivenhain, Rainbow, Rancho Santa Fe, San Marcos, Santa Ysabel, Solana Beach, Valley Center, Vista, and Warner Springs</td>
<td>San Diego Field Office</td>
<td>10385 Vista Sorrento Parkway, San Diego, CA 92121</td>
<td>(858) 320-1800</td>
</tr>
</tbody>
</table>
## FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>California</td>
<td>San Francisco and San Mateo, Contra Costa, Del Norte and Humboldt, Monterey and Santa Cruz, Alameda, San Jose and Santa Clara, Lake, Marin, Sonoma, and Napa.</td>
<td>San Francisco Field Office</td>
<td>450 Golden Gate Avenue, 13th Floor, San Francisco, CA 94102-9523</td>
<td>(415) 553-7400</td>
</tr>
<tr>
<td>Colorado</td>
<td>all counties</td>
<td>Denver Field Office</td>
<td>8000 East 36th Avenue Denver, CO 80238</td>
<td>(303) 629-7171</td>
</tr>
<tr>
<td>Connecticut</td>
<td>all counties</td>
<td>New Haven Field Office</td>
<td>600 State Street, New Haven, CT 06511</td>
<td>(203) 777-6311</td>
</tr>
<tr>
<td>Florida</td>
<td>City of Miami, North Miami Beach, West Palm Beach, Homestead, Fort Pierce and Key West.</td>
<td>Miami Field Office</td>
<td>2030 SW 145th Avenue, Miramar, FL 33027</td>
<td>(754) 703-2000</td>
</tr>
<tr>
<td>Florida</td>
<td>City of Tampa, Lakeland, Orlando, Brevard, Pinellas, Ft. Meyers, Sarasota and Naple.</td>
<td>Tampa Field Office</td>
<td>5525 West Gray Street, Tampa, FL 33609</td>
<td>(813) 253-1000</td>
</tr>
<tr>
<td>Georgia</td>
<td>all counties</td>
<td>Atlanta Field Office</td>
<td>3000 Flowers Road S Atlanta, GA 30341</td>
<td>(770) 216-3000</td>
</tr>
<tr>
<td>Guam</td>
<td>all counties</td>
<td>Honolulu Field Office</td>
<td>91-1300 Enterprise Street Kapolei, HI 96707</td>
<td>(808) 566-4300</td>
</tr>
<tr>
<td>Hawaii</td>
<td>all counties</td>
<td>Honolulu Field Office</td>
<td>91-1300 Enterprise Street Kapolei, HI 96707</td>
<td>(808) 566-4300</td>
</tr>
<tr>
<td>Illinois</td>
<td>JoDavies, Stephenson, Winnebago, Boone, McHenry, Lake, Carroll, Ogle, Dekalb, Kane, Dupage, Cook, Whiteside, Lee, Kendall, Will, and Grundy, LaSalle</td>
<td>Chicago Field Office</td>
<td>2111 W. Roosevelt Road Chicago, IL 60608</td>
<td>(312) 421-6700</td>
</tr>
</tbody>
</table>
### FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Illinois</td>
<td>Adams, Brown, Cass, Christian, Green, Logan, Macoupin, Mason, Menard, Montgomery,</td>
<td>Springfield Field</td>
<td>900 East Linton Avenue, Springfield, IL 62703</td>
<td>(217) 522-9675</td>
</tr>
<tr>
<td></td>
<td>Morgan, Pike, Sangamon, Schuyler, and Scott, Champaign, Coles, DeWitt, Douglas,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Edgar, Ford, Iroquois, Kankakee, Macon, Moultrie, Piatt, Shelby, and Vermilion,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bond, Calhoun, Clark, Clinton, Crawford, Cumberland, Effingham, Fayette, Jasper,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Jersey, Madison, Marion, Monroe, Randolph, St. Clair, and Washington, Alexander,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clay, Edwards, Franklin, Gallatin, Hamilton, Hardin, Jackson, Jefferson, Johnson,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Lawrence, Massac, Pope, Pulaski, Richland, Saline, Union, Wabash, Wayne, White,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>and Williamson, Fulton, Hancock, Livingston, Marshall, McDonough, McLean, Peoria,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Putnam, Tazewell, and Woodford, Bureau, Henderson, Henry, Knox, Mercer, Rock Island,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stark, and Warren.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Indiana</td>
<td>all counties</td>
<td>Indianapolis Field</td>
<td>8825 Nelson B Klein Pkwy Indianapolis, IN 46250</td>
<td>(317) 595-4000</td>
</tr>
<tr>
<td>Iowa</td>
<td>all counties</td>
<td>Omaha Field Office</td>
<td>4411 South 121st Court, Omaha, NE 68137-2112</td>
<td>(402) 493-8688</td>
</tr>
<tr>
<td>Kansas</td>
<td>all counties</td>
<td>Kansas City Field</td>
<td>1300 Summit Street, Kansas City, MO 64105</td>
<td>(816) 512-8200</td>
</tr>
<tr>
<td>Kentucky</td>
<td>all counties</td>
<td>Louisville Field</td>
<td>12401 Sycamore Station Place, Louisville, KY 40299-6198</td>
<td>(502) 263-6000</td>
</tr>
<tr>
<td>Louisiana</td>
<td>all counties</td>
<td>New Orleans Field</td>
<td>2901 Leon C. Simon Boulevard, New Orleans, LA 70126</td>
<td>(504) 816-3000</td>
</tr>
<tr>
<td>Maine</td>
<td>all counties</td>
<td>Boston Field Office</td>
<td>201 Maple Street Chelsea, MA 02150</td>
<td>(857) 386-2000</td>
</tr>
<tr>
<td>Maryland</td>
<td>Baltimore (including Baltimore City), Howard, Baltimore (including Baltimore City),</td>
<td>Baltimore Field</td>
<td>2600 Lord Baltimore Drive, Baltimore, MD 21244</td>
<td>(410) 265-8080</td>
</tr>
<tr>
<td></td>
<td>Howard, Anne Arundel, Calvert, Charles, Kent, Queen Anne’s, and St. Mary’s, Harford,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Allegany, Carroll, Frederick, Garrett, and Washington, Prince George’s, Montgomery,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Caroline, Dorchester, Somerset, Talbot, Worcester, and Wicomico, Kent, Sussex, and New Castle.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Cities and County</td>
<td>FBI Field Office</td>
<td>Address</td>
<td>Phone</td>
</tr>
<tr>
<td>-------------</td>
<td>-----------------------------------------------------------------------------------</td>
<td>--------------------</td>
<td>----------------------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Massachusetts</td>
<td>all counties</td>
<td>Boston Field Office</td>
<td>201 Maple Street Chelsea, MA 02150</td>
<td>(857) 386-2000</td>
</tr>
<tr>
<td>Michigan</td>
<td>all counties</td>
<td>Detroit Field Office</td>
<td>477 Michigan Ave., 26th Floor Detroit, MI 48226</td>
<td>(313) 965-2323</td>
</tr>
<tr>
<td>Minnesota</td>
<td>all counties</td>
<td>Minneapolis Field Office</td>
<td>1501 Freeway Boulevard, Brooklyn Center, MN 55430</td>
<td>(763) 569-8000</td>
</tr>
<tr>
<td>Mississippi</td>
<td>all counties</td>
<td>Jackson Field Office</td>
<td>1220 Echelon Parkway, Jackson, MS 39213</td>
<td>(601) 948-5000</td>
</tr>
<tr>
<td>Missouri</td>
<td>City of St. Louis, Jefferson, St. Louis, Cape Girardeau,</td>
<td>St. Louis Field Office</td>
<td>2222 Market Street, St. Louis, MO 63103</td>
<td>(314) 589-2500</td>
</tr>
<tr>
<td></td>
<td>Bollinger, Butler, Carter, Dunklin, Iron, Madison, Mississippi,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>New Madrid, Pemiscott, Perry, Reynolds, Ripley, Scott,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shannon, St. Francois, Ste. Genevieve, Stoddard, Wayne,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Audrain, Clark, Lewis, Marion, Monroe, Pike, Ralls, Adair,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Chariton, Knox, Linn, Macon, Rnadolph, Schuyler, Scotland,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Shelby, Crawford, Dent, Franklin, Gasconade, Maries,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Phelps, Washington, Lincoln, Montgomery, St. Charles, and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Warren.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Missouri</td>
<td>Barry, Barton, Bourbon, Cherokee, Crawford, Dade, Jasper,</td>
<td>Kansas City Field Office</td>
<td>1300 Summit Street, Kansas City, MO 64105</td>
<td>(816) 512-8200</td>
</tr>
<tr>
<td></td>
<td>Labette, Lawrence, McDonald, Newton, Vernon, Cass, Clay,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Bates, Jackson, Johnson, Leavenworth, Linn, Miami, Platte,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Ray, Wyandotte, Andrew, Atchison, Buchanan, Caldwell,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Clinton, Davies, DeKalb, Gentry, Grundy, Harrison, Holt,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Mercer, Nodaway, Putnam, Sullivan, Worth, Benton,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Cedar, Christian, Dallas, Douglas, Greene, Henry, Hickory,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Howell, Laclede, Oregon, Ozark, Polk, Pulaski, St. Clair,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Stone, Taney, Texas, Webster, Wright, Boone, Callaway,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Camden, Carroll, Cole, Cooper, Howard, Johnson, Lafayette,</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Livingston, Miller, Moniteau, Morgan, Osage, Pettis, and</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Saline.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Montana</td>
<td>all counties</td>
<td>St. Lake City Field Office</td>
<td>5425 West Amelia Earhart Drive, Salt Lake City, UT 84116</td>
<td>(801) 579-1400</td>
</tr>
<tr>
<td>Nebraska</td>
<td>all counties</td>
<td>Omaha Field Office</td>
<td>4411 South 121st Court, Omaha, NE 68137-2112</td>
<td>(402) 493-8688</td>
</tr>
</tbody>
</table>
Exhibit A — 5/9

FBI contact information by jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Hampshire</td>
<td>all counties</td>
<td>Boston Field Office</td>
<td>201 Maple Street Chelsea, MA 02150</td>
<td>(857) 386-2000</td>
</tr>
<tr>
<td>New Mexico</td>
<td>Counties and cities covered: Alexandria, Arlington, Fairfax (county and city), Falls Church, Fauquier, Leesburg, Loudon, Manassas, Prince William, Quantico, Vienna, and Warrenton.</td>
<td>Albuquerque Field Office</td>
<td>4200 Luecking Park Avenue NE, Albuquerque, NM 87107</td>
<td>(505) 889-1300</td>
</tr>
</tbody>
</table>
### FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>North Carolina</td>
<td>all counties</td>
<td>Charlotte Field Office</td>
<td>7915 Microsoft Way Charlotte, NC 28273</td>
<td>(704) 672-6100</td>
</tr>
<tr>
<td>North Dakota</td>
<td>all counties</td>
<td>Minneapolis Field Office</td>
<td>1501 Freeway Boulevard, Brooklyn Center, MN 55430</td>
<td>(763) 569-8000</td>
</tr>
<tr>
<td>Oklahoma</td>
<td>all counties</td>
<td>Oklahoma City Field Office</td>
<td>3301 West Memorial Road, Oklahoma City, OK 73134-7098</td>
<td>(405) 290-7770</td>
</tr>
<tr>
<td>Oregon</td>
<td>all counties</td>
<td>Portland Field Office</td>
<td>9109 NE Cascade Parkway, Portland, OR 97220</td>
<td>(503) 224-4181</td>
</tr>
</tbody>
</table>
## FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>Bureau Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rhode Island</td>
<td>all counties</td>
<td>Boston Field Office</td>
<td>201 Maple Street Chelsea, MA 02150</td>
<td>(857) 386-2000</td>
</tr>
<tr>
<td>South Dakota</td>
<td>all counties</td>
<td>Minneapolis Field Office</td>
<td>1501 Freeway Boulevard, Brooklyn Center, MN 55430</td>
<td>(763) 569-8000</td>
</tr>
<tr>
<td>Tennessee</td>
<td>Shelby Fayette, Tipton, Lauderdale, Dyer, Lake, obion, Weakly, Gibson, Crockatt, Haywood, Madison, Hardeman, Henry, Carroll, Henderson, Chester, McNairy, Hardin, Decatur, Benton, Stewart, Houston, Humphreys, Perry, Wayne, Montgomery, Dickson, Hickman, Lewis, Lawrence, Cheatham, Robertson, Davidson, Williamson, Maury, Giles, Sumner, Trousdale, Rutherford, Marshall, Wilson, Smith, Macon, Canon, DeKalb, Smith, Jackson, Clay, Putnam, Overton, Pickett, Fentress, and Cumberland.</td>
<td>Memphis Field Office</td>
<td>225 North Humphreys Boulevard, Suite 3000, Memphis, TN 38120</td>
<td>(901) 747-4300</td>
</tr>
</tbody>
</table>
## FBI Field Offices and Jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>Texas</td>
<td>Madison, Brazos, Grimes, Walker, San Jacinto, Liberty, Hardin, Jasper, Newton, Orange, Jefferson, Montgomery, Waller, Harris, Chambers, Fayette, Austin, Colorado, Fort Bend, Galveston, Brazoria, Wharton, Matagorda, Lavaca, DeWitt, Jackson, Victoria, Goliad, Refugio, Bee, San Patricio, Live Oak, Jim Wells, Arkansas, Nueces, Kleberg, Kennedy, Brooks, and Duval.</td>
<td>Houston Field Office</td>
<td>1 Justice Park Drive Houston, TX 77292</td>
<td>(713) 693-5000</td>
</tr>
<tr>
<td>Texas</td>
<td>Cities of Abilene, Amarillo, DFW Airport, Fort Worth, Lubbock, Lufkin, Plano, San Angelo, Sherman, Texarkana, Tyler, Wichita Falls.</td>
<td>Dallas Field Office</td>
<td>One Justice Way Dallas, TX 75220</td>
<td>(972) 559-5000</td>
</tr>
<tr>
<td>Texas</td>
<td>Brewster, Jeff Davis, Pecos, Reeves, and Presidio, Andrews, Crane, Ector, Loving, Martin, Midland, Upton, Ward, and Winkler.</td>
<td>El Paso Field Office</td>
<td>El Paso Federal Justice Center, 660 South Mesa Hills Drive, El Paso, TX 79912</td>
<td>(915) 832-5000</td>
</tr>
<tr>
<td>Utah</td>
<td>all counties</td>
<td>St. Lake City Field Office</td>
<td>5425 West Amelia Earhart Drive, Salt Lake City, UT 84116</td>
<td>(801) 579-1400</td>
</tr>
<tr>
<td>Vermont</td>
<td>all counties</td>
<td>Albany Field Office</td>
<td>200 McCarty Avenue Albany, NY 12209</td>
<td>(518) 465-7551</td>
</tr>
<tr>
<td>Virgin Islands</td>
<td>all counties</td>
<td>San Juan Field Office</td>
<td>Federal Office Building, Suite 526, 150 Carlos Chardon Avenue, Hato Rey, PR 00918</td>
<td>(787) 754-6000</td>
</tr>
<tr>
<td>Virginia</td>
<td>Accomack, Chesapeake, Eastern Shore, Norfolk, Northhampton, Portsmouth, Suffolk, Virginia Beach, Gloucester, Hampton, Isle of Wight, James City County, Mathews, Newport News, Mathews, Poquoson, Southampton, Williamsburg, and York County.</td>
<td>Norfolk Field Office</td>
<td>509 Resource Row, Chesapeake, VA 23320</td>
<td>(757) 455-0100</td>
</tr>
</tbody>
</table>
## FBI contact information by jurisdiction

<table>
<thead>
<tr>
<th>State</th>
<th>Cities and County</th>
<th>FBI Field Office</th>
<th>Address</th>
<th>Phone</th>
</tr>
</thead>
<tbody>
<tr>
<td>West Virginia</td>
<td>all counties</td>
<td>Pittsburgh Field Office</td>
<td>3311 East Carson Street, Pittsburgh, PA 15203</td>
<td>(412) 432-4000</td>
</tr>
<tr>
<td>Wisconsin</td>
<td>all counties</td>
<td>Milwaukee Field Office</td>
<td>3600 S. Lake Drive, St. Francis, WI 53235</td>
<td>(414) 276-4684</td>
</tr>
<tr>
<td>Wyoming</td>
<td>all counties</td>
<td>Denver Field Office</td>
<td>8000 East 36th Avenue Denver, CO 80238</td>
<td>(303) 629-7171</td>
</tr>
</tbody>
</table>
Exhibit B

Sample pleadings to obtain an ex-parte injunctive order preventing a financial institution from allowing funds to be transferred from an account that includes your funds
EXHIBIT B

SAMPLE PLEADINGS TO OBTAIN AN EX-PARTE INJUNCTIVE ORDER PREVENTING A FINANCIAL INSTITUTION FROM ALLOWING FUNDS TO BE TRANSFERRED FROM AN ACCOUNT THAT INCLUDE YOUR FUNDS.

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE.

THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED.

LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
STATE OF ______________ [INSERT NAME OF COURT]

[INSERT COMPANY NAME], a [INSERT STATE OF INCORPORATION] company, Case No. [INSERT DOCKET PREFIX]

                      Plaintiff,                              Hon.
v. 

JOHN DOE, an individual, and JANE DOE, an individual, jointly and severally, and                     

_________________ BANK, a ____________________ Corporation,

                     Defendants,

[INSERT LEGAL COUNSEL INFORMATION]

________________________________________________________

VERIFIED COMPLAINT

There is no other pending or resolved civil action arising out of the same transaction or occurrence as alleged in this Complaint.

Plaintiff [INSERT COMPANY NAME] (“Plaintiff”) for their Complaint against John Doe, Jane Doe and _______ Bank (collectively “Defendants”) state as follows:

PARTIES

1. Plaintiff is a corporation doing business in the State of _________.

2. Defendant John Doe is an individual residing in __________, __________.

3. Defendant Jane Doe is an individual residing in __________, __________.

4. Defendant _______ Bank is a ______________ company doing business in __________ County, __________.

JURISDICTION AND VENUE

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
5. This Court has subject matter jurisdiction over this civil action pursuant to [SITE STATUTORY AUTHORITY FOR JURISDICTION].

6. The action involves an amount in controversy in excess of $___________, exclusive of interest and costs.

7. This Court has personal jurisdiction over Defendants because they reside and/or conduct business in the County of __________, State of ________________.

**General Allegations**

8. Plaintiff incorporates by reference and restates all allegations above as though fully set forth herein.

9. On ___________, 20__, Defendants John and Jane Doe received a wire transfer of $________ in error from ______ Bank. (See Redacted Account Information attached as Exhibit __).

10. The funds received in John and Jane Doe’s account was transferred in error. (See Sworn Affidavit of __________ attached as Exhibit __).

11. The funds were incorrectly transferred from a real estate closing transaction that occurred on ____________.

12. _________ Bank has possession of the funds and has the power to freeze the funds until this matter is voluntarily resolved or addressed by further order of this Court.

**Count I**

**Unjust Enrichment**

13. Plaintiff incorporates by reference and restates all allegations above as though fully set forth herein.

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
14. Defendants received $______ by means of a wire transfer that was incorrectly directed to their account.

15. The funds received by Defendants belong to _________ and Defendants have no proper or legal claim to the funds.

16. Defendants have been unjustly enriched by receiving the funds without legal or equitable right to the funds.

17. It would be inequitable to allow Defendants to retain the funds or to exercise any dominion or control over the funds.

WHEREFORE, Plaintiff seeks a judgment against Defendant so that it may reclaim and properly disburse the funds wired to Defendants' account in error.

Respectfully submitted,

[INSERT LAW FIRM NAME]

BY: __________________________
[INSERT ATTORNEY NAME AND CONTACT INFORMATION]

DATED: ____________, 20__

Verification

The allegations in this Complaint are accurate to the best of my knowledge and belief.

[INSERT NAME OF COMPANY OFFICER OR OWNER VERIFYING THE FACTS ALLEGED]
Subscribed and sworn before me
this ___ day of ________________, 20__.

______________________________
Notary Public, ____________ County, ____________
Acting in ____________ County, ____________
My Commission Expires: ________________

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
STATE OF _____

COUNTY OF _____

AFFIDAVIT OF [INSERT NAME OF PERSON PROVIDING INFORMATION]

[INSERT NAME OF PERSON PROVIDING INFORMATION] being duly sworn, deposes
and states:

1. I am [INSERT STATE OF RESIDENCY] and I am over the age of 18.

2. I am the [INSERT COMPANY POSITION] of [INSERT COMPANY NAME] and my
business address is [INSERT COMPANY ADDRESS].

3. If sworn as a witness, I can testify competently to the facts stated herein.

4. [INSERT FACTS DESCRIBING THE LOSS]
5. [INSERT FACTS DESCRIBING THE LOSS]
6. [INSERT FACTS DESCRIBING THE LOSS]

DATED: ______________, 20__

[INSERT NAME OF SIGNATORY]
[INSERT NAME OF COMPANY]
Its: [INSERT TITLE]

Subscribed and sworn before me
this __ day of ____________, 20__.

______________________________
Notary Public, ____________ County, ____________
Acting in ____________ County, ____________
My Commission Expires: ________________

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND
EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT
GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED
WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE
ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS
EXHIBIT B.
STATE OF
[INSERT NAME OF COURT]

[INSERT COMPANY NAME],
a [INSERT STATE OF INCORPORATION] company. Case No. [INSERT DOCKET PREFIX]

Plaintiff,

v.

JOHN DOE, an individual, and JANE DOE, an individual, jointly and severally, and

BANK, a Corporation,

Defendants,

[INSERT LEGAL COUNSEL INFORMATION]

EX PARTE MOTION FOR TEMPORARY RESTRAINING ORDER & PRELIMINARY INJUNCTION

Plaintiff, [INSERT COMPANY NAME] ("Plaintiff") pursuant to [INSERT CITATION FOR AUTHORITY TO GRANT THE ORDER] for entry of a Temporary Restraining Order states as follows:

Plaintiff relies upon and incorporates its Brief in Support of the Motion (the "Brief") filed contemporaneously herewith.

WHEREFORE, Plaintiff, [INSERT COMPANY NAME], respectfully requests that this Court enter an Ex Parte Temporary Restraining Order freezing $__________ that was transferred in error to John and Jane Doe’s bank account at ___________ Bank.

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
STATE OF
[INSERT NAME OF COURT]

[INSERT COMPANY NAME], a
[INSERT STATE OF INCORPORATION] company, Case No. [INSERT DOCKET
PREFIX]

Plaintiff,

v.

JOHN DOE, an individual, and JANE DOE,
an individual, jointly and severally, and
BANK, a
Corporation,

Defendants,

[INSERT LEGAL COUNSEL INFORMATION]

PLAINTIFF’S BRIEF IN SUPPORT OF EX PARTE MOTION FOR
TEMPORARY RESTRAINING ORDER

Plaintiff, [INSERT COMPANY NAME] ("Plaintiff") pursuant to [INSERT
APPLICABLE STATE COURT RULE ALLOWING FOR SUCH RELIEF] for entry of a
Temporary Restraining Order states as follows for its Brief in Support:

1. Relevant Facts

On [INSERT NAME], Defendants John and Jane Doe received a wire transfer of
$__________ in error from ________ Bank. (See Redacted Account Information attached as
Exhibit __). The funds received in John and Jane Doe’s account were transferred in error. (See
Sworn Affidavit of __________ attached as Exhibit __). The funds were incorrectly transferred
from a real estate closing transaction that occurred on ______________. __________

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND
EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT
GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED
WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE
ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS
EXHIBIT B.
Bank has possession of the funds and has the power to freeze the funds until this matter is voluntarily resolved or addressed by further order of this Court.

II. Law & Analysis

An ex parte temporary restraining order is justified in this case because immediate and irreparable injury, loss or damage will result from the delay required to effect notice. (See Sworn Affidavit of ________ attached as Exhibit __). Furthermore, notice itself may precipitate adverse action with respect to the improperly transferred funds before an order can be issued. [INSERT CITIATION FOR AUTHORITY].

Plaintiff has provided notice to ________ Bank on ________ consistent with [INSERT CITATION FOR NOTICE REQUIREMENT]. Plaintiff has attempted to identify the owners of the account but has been unable to do so, given banking privacy regulations. ________ Bank has not voluntarily returned or frozen the funds thereby necessitating this Motion.

The temporary restraining order and injunctive relief are justified where the movant can establish: [INSERT THE ELEMENTS NECESSARY TO OBTAIN A RESTRAINING ORDER AND INJUNCTIVE RELIEF. THE ELEMENTS 1-4 BELOW ARE THE ELEMENTS REQUIRED IN THE STATE OF MICHIGAN.]

(1) a likelihood of success on the merits;

(2) immediate and irreparable injury will result without the issuance of an injunction;

(3) a balance of harm to the Plaintiff relative to the Defendant if injunctive relief is denied; and

(4) the public interest will not be harmed by issuance of the injunction.

[INSERT STATUTORY OR CASE LAW PROVIDING AUTHORITY FOR THE RELIEF AND ELEMENTS REQUIRED TO OBTAIN RELIEF]
[THE SECTIONS BELOW INCLUDE SAMPLE LANGUAGE AND CASE CITATIONS USED IN MICHIGAN TO SUBSTANTIATE EACH OF THE FOUR ELEMENTS REQUIRED TO OBTAIN THE RELIEF REQUESTED. THIS WILL NEED TO BE TAILORED TO THE LAWS AND REQUIREMENTS IN EACH APPLICABLE STATE]

It is not necessary that the complainant's rights be clearly established, or that the court find complainant is entitled to prevail on the final hearing. It is sufficient if it appears that there is a real and substantial question between the parties, proper to be investigated in a court of equity, and in order to prevent irreparable injury to the complainant, before his claims can be investigated, it is necessary to prohibit any change in the conditions and relations of the property and of the parties during the litigation." Niedzialek v Journeymen Barbers, Hairdressers & Cosmetologists' Intern Union of America, Local No. 552 (AFL), 331 Mich 296, 302; 49 NW2d 273 (1951) (citations omitted).

A. There is a substantial likelihood of Plaintiff's success on the merits.

Plaintiff has clearly stated its claim for unjust enrichment and has demonstrated that Defendants have no right, title or interest in the funds. Plaintiff has established the source of the funds and the intended recipient with admissible sworn testimony. It would be unjust and inequitable for Defendants to retain the benefit of the transferred funds. Plaintiff is likely, if not assured, to prevail on the merits of its claim. There is no conceivable defense or justification for opposing the requested relief.

B. Without injunctive relief Plaintiff will suffer irreparable injury.

"It is the settled policy of this Court under such circumstances to grant to a litigant who is threatened with irreparable injury temporary injunctive relief and thereby preserve the original status quo." Niedzialek v Journeymen Barbers, Hairdressers & Cosmetologists' Intern Union of

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND EDUCATIONAL PURPOSES ONLY AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE. THE INFORMATION IS NOT GUARANTEED TO BE CORRECT, COMPLETE OR CURRENT. CERTIFID LLC MAKES NO EXPRESS OR IMPLIED WARRANTY ABOUT THE ACCURACY OR RELIABILITY OF THE INFORMATION PROVIDED. LEGAL COUNSEL MUST BE ENGAGED PRIOR TO TAKING ANY ACTIONS SUGGESTED OR IMPLIED BY THE INFORMATION PROVIDED IN THIS EXHIBIT B.
America, Local No. 552 (AFL), 331 Mich 296; 49 NW2d 273 (1951). "In order to establish irreparable injury, the moving party must demonstrate a noncompensable injury for which there is no legal measurement of damages or for which damages cannot be determined with a sufficient degree of certainty." Thermostool Corp v Borzym, 227 Mich App 366; 575 NW2d 334 (1998).

"[A]n injury is irreparable where the damages are estimable only by conjecture and not by accurate standard." Ainsworth v Hunting and Fishing Club, 153 Mich 185, 191; 116 NW 992 (1908).

Plaintiff will also suffer irreparable harm if the funds are not frozen. The funds transferred in error are a significant sum and will be difficult if not impossible to efficiently recover the funds if they are intentionally or unintentionally lost or depleted. Plaintiff simply seeks to preserve the status quo to avoid damages, fees and the expense of litigation if the funds are not immediately frozen.

C. The balancing of harms favors Plaintiff.

The balance of harm weighs in favor of granting Plaintiff’s request for a temporary restraining order and injunctive relief. Defendants have no right to the funds received in their account and will experience no harm or prejudice if those funds are frozen pending resolution of this dispute. On the other hand, the harm facing Plaintiff and the proper owner of the funds are subject to losses, damages, fees and expenses that are certain to occur if the funds are lost or depleted in any way. Plaintiff is unaware of any third party that would be affected by the requested relief.

D. The requested relief will further the public interest.
The public has an interest in preserving the status quo during the pendency of this dispute to properly direct the funds to the party that has proper legal interest in the money. The public interest is not served by allowing funds incorrectly transferred to be lost or depleted, internationally or otherwise, when the party receiving the funds has not right, title or interest in the funds.

III. Conclusion

For all the reasons discussed above, Plaintiff has established the requirements for an ex parte temporary restraining order and a preliminary injunction and requests that this Court enter the Proposed Ex Parte Temporary Restraining Order attached a Exhibit __ ordering (1) ________ Bank to immediately freeze $_________. that was improperly transferred to Defendants’ account, (2) restrict Defendants from accessing, transferring or otherwise impacting the $_________ without Plaintiff’s written authorization, (3) Defendants to show cause on __________ why a preliminary injunction should not issue, and (4) grant Plaintiff such other and further relief as the Court deems appropriate.

Respectfully submitted,

[INSERT LAW FIRM NAME]

BY: [INSERT ATTORNEY NAME AND CONTACT INFORMATION]

DATED: _____________, 20__
EXHIBIT B - SAMPLE

STATE OF  
[INSERT NAME OF COURT]

[INSERT COMPANY NAME], a  
[INSERT STATE OF INCORPORATION] company,  

Case No. [INSERT DOCKET PREFIX]

Plaintiff,

v.

JOHN DOE, an individual, and JANE DOE,  
an individual, jointly and severally, and  

BANK, a  
Corporation,

Defendants,

[INSERT LEGAL COUNSEL INFORMATION]

EX PARTE TEMPORARY RESTRAINING ORDER  
At a session of said Court held in the [INSERT COURT NAME AND LOCATION],

: ___ AM/PM

PRESENT: HON.  
[INSERT JUDGE’S TITLE]

Having considered the proofs and arguments of Plaintiff’s counsel during an ex parte  
hearing on _________, 20___, this Court now finds that irreparable harm would likely  
 occur to Plaintiff in the form of loss or depletion of $_______ that was improperly  
 transferred to John and Jane Doe’s bank account held at _______________ Bank. The  
 Court is also satisfied that the requirements of [INSERT CITATION OF AUTHORITY FOR  
GRANTING THE ORDER] have been satisfied given the immediate need to isolate and preserve  
the transferred funds.

LEGAL DISCLAIMER: THE INFORMATION CONTAINED IN THIS EXHIBIT B IS PROVIDED FOR INFORMATIONAL AND  
educational purposes only and should not be construed as legal advice. The information is not  
guaranteed to be correct, complete or current. CERTIFID LLC makes no express or implied  
 warranty about the accuracy or reliability of the information provided. Legal counsel must be  
engaged prior to taking any actions suggested or implied by the information provided in this  
exhibit B.
IT IS HEREBY ORDERED that ______ Bank is to immediately freeze $______ that was improperly transferred to Defendants’ account and Defendants are restricted from accessing, transferring or otherwise impacting the $______ without Plaintiff’s written authorization;

IT IS FURTHER ORDERED that Defendants are to show cause on __________, 20__ why a preliminary injunction extending the relief provided in this Order should not issue.

DATED:_________ __________ Hon.
Exhibit C

Data Security and Best Practices Guide
Data security encompasses a wide variety of practices, methods, and procedures based on the type of organization, technology topology (on-premises, cloud, or hybrid) and type of data being protected. While not all of these combinations can be accounted for in a single document, there are general concepts that can help direct the planning process for any organization. These practices can be divided in terms of Systems, People, and Processes which can address the confidentiality, integrity and availability of systems and data.

All the practices below should be put into the context of standards. The most popular standards in the market place today can help guide you through the implementation of your security program and ensure the right security posture for your organization. While not comprehensive, below are some of the most popular standards in use today:

- ISO/IEC 27001 - Information security management systems
- NIST Cyber Security Framework
- NIST Small Business Security (The Fundamentals)
- Center for Internet Security – Best Practices
- ISACA - Control Objectives for Information and Related Technologies (COBIT)
- Open Web Application Security Project (OWASP)
- Information Technology Infrastructure Library (ITIL)

While the list below is not exhaustive its purpose is to show the base building blocks of controls that should be in place to ensure a sound and secure environment. For expanded views into other controls, review the ISO 27002 and NIST 800-53 control documents which go into much greater detail and explanation.
Systems

Perimeter
Appliances such as firewalls, routers, and specialized equipment for Intrusion Detection, Log Monitoring and Artificial Intelligence (AI) can all play a role in hardening an environment such as:

- Web content filtering
- Anti-virus scanning
- Reputation, application, and protocol protection
- Advanced threat protection for zero-day exploits
- Data loss prevention and auditing policies
- Deep Packet Inspection of HTTPS traffic
- Geolocation-based blocking
- Intrusion detection

Wireless security
- Identity-based 802.1x authentication
- Wireless intrusion prevention
- Properly separated guest, employee and production networks
- Mobile device management

Systems monitoring
- Collection of logs at every critical point in the network, including firewall/router and front-end and back-end systems
- Security monitoring and alerting based on smart triggers
- Use of AI to spot hard to see intrusion and data exfiltration attempts

Infrastructure
- Redundant, robust, and encrypted backup strategy including cloud and other off-premise backups
- Data classification
- Data encryption at rest and in transit
- Data tokenization
- Email digital signatures
- Email encryption
- Use industry leading spam, malware, and virus filters, to filter and protect against spam, viruses, phishing, and malicious attachments
- Enable two-factor authentication to domain registrar, DNS, and other hosting environments
- Implement DNSSEC to ensure that DNS records cannot be compromised or taken over
- DKIM and SPF record to protect against malicious domain spoofing
- Ensure OS and third party applications are patched according to vendor recommendations
People

Perimeter

- Train employees to be aware of anything that might look different outside of their normal world. This can include email, phone, other forms of communication, or people without proper identification. Train with real examples to make a strong impact. Red team exercises are also beneficial.
- Never enter login information outside of the normal outlets, especially email.
- Don’t open unexpected, unsolicited, or suspicious attachments. Always verify with IT when possible.
- Ensure data is saved to trusted network/server locations and do not allow USB storage devices.
- Conduct unannounced phishing testing on a periodic basis using a trusted, third party firm.
- Conduct and track regular training of employees using a trusted, third party firm.
- Prevent “Shadow IT” cloud services by auditing access logs, financial records, and user behavior.
- Ensure all users have access to and have read and acknowledge security policy documents.

Physical

- Locked doors with proper access to employee and infrastructure areas.
- Clean desk policies.
- Proper identification for staff and vendors.
- Security cameras.
Processes

Access controls
• Role-based file permissions
• File system and application specific permissions
• Dedicated service accounts to isolate access to critical systems if one is compromised
• Least privileged accounts with minimum required access
• Complex, yet enforceable, user password policies
• Multi-factor authentication
• VPN connections for remote users
• Penetration testing utilizing services

Client and endpoint security
• Software restriction policies
• Removing administrator permissions from users
• Regular antivirus scans and reporting

Infrastructure
• Disaster recovery and incident response planning
• Emergency preparedness for natural and manmade events

Audits
• Conduct scheduled internal audits of your security program to determine any actions that need to be taken to remediate the program. A plan that includes the: DO, CHECK, and ACT process can help you continuously monitor and improve your security stance
• Conduct annual external audits led by third parties to ensure compliance with best practices and current standards
• Conduct third party risk assessments on all vendors annually or more frequently as the business process requires