Fraud Prevention Highlights & Training Guide

(CPB Rising Tide Webinar: **Protect What You've Built: Practical Fraud Prevention for Hawaii Businesses**)

WHAT EVERY BUSINESS SHOULD REMEMBER

Fraud is a business risk

Criminal groups operate like businesses. Smaller businesses are now primary targets, especially as AI makes scams more convincing.

The human element matters

Technology enables fraud, but often people are the control point. Social engineering, urgency, trust, and emotional manipulation often make it successful.

Speed matters

If fraud happens, contact your bank immediately. Recovery odds can drop sharply after the first 72 hours.

USE THIS PAUSE-AND-VERIFY CHECKLIST BEFORE MONEY OR INFORMATION MOVES

1. Reconnaissance: Limit public personal/business details. Use privacy settings and monitor for company data in breach databases.	**2. Targeting & prep:** Check sender addresses and domains carefully. Be skeptical of urgent requests. Never trust caller ID alone.
3. Initial contact: Pause before responding. Do not click unsolicited links. Contact the organization using known numbers.	**4. Exploitation:** Use strong unique passwords, a password manager, MFA, updated devices, and dual approval for transactions.
5. Persistence: Review account activity, password changes, email forwarding/filter rules, and set account alerts wherever possible.	**6. Financial strike:** Use Positive Pay, ACH Positive Pay where available, transaction limits, daily transfer limits, and monthly reconciliations.
7. Cover-up: Report suspicious activity quickly. Preserve evidence, document what happened, and file with IC3/law enforcement as appropriate.	**Team habit:** Normalize questions and call-back verification. Build a culture where employees are expected to slow down and verify.

PRACTICAL CONTROLS TO PUT IN PLACE

Payment protections

- Checks: hand deliver when possible, mail inside the post office, follow up with the payee, and timely review bank statements.
- Enroll in Check Positive Pay; consider ACH/wires/online platforms/corporate cards when appropriate.
- Use dual approval for payments and set transaction or daily transfer limits.

Cyber hygiene

- Use a password manager and strong, unique passwords; enable MFA with distinct factors.
- Do not share remote access to devices. Keep antivirus, security software, and patches up to date.
- Do not mix work and personal accounts/devices. Train employees and consider cyber insurance.

CENTRAL PACIFIC BANK

Member FDIC

Fraud Response & Resource Guide

IF FRAUD IS SUSPECTED: FIRST 24 HOURS

1. Stop	2. Secure	3. Document	4. Report
Stop payment, recall wires, freeze access, and contact your financial institutions immediately.	Change passwords, revoke access, preserve devices/logs, and check email settings.	Save emails, texts, call logs, screenshots, payment details, account numbers, and timelines.	File reports with your financial institution, law enforcement, and the appropriate agencies below.

WHERE TO REPORT SUSPECTED FRAUD

Your financial institutions
Call the trusted number on your bank's website or on your card.

FBI Internet Crime Complaint Center (IC3) | www.ic3.gov
Report cyber-enabled crime, business email compromise, online fraud, ransomware, and internet scams.

FBI Honolulu Field Office | https://tips.fbi.gov/home
24/7 local FBI contact: (808) 566-4300.
Tips can also be submitted online.

FTC ReportFraud.gov | reportfraud.ftc.gov
Report fraud, scams, or bad business practices.

FTC IdentityTheft.gov | www.identitytheft.gov
Report identity theft and create a recovery plan.
Phone: 1-877-438-4338

RESOURCES FOR SMALL BUSINESSES

Global Cyber Alliance | https://gcatoolkit.org/smallbusiness/
Free cybersecurity tool kit and learning portal.

Cybersecurity & Infrastructure Security Agency | https://www.cisa.gov/audiences/small-and-medium-businesses
Information and tools to help businesses protect their people, customers, IP and other sensitive data and physical threats.

Federal Trade Commission | https://www.ftc.gov/business-guidance/small-businesses
Resources to help you avoid scams, protect your computers and networks, keep your customers' data safe, and protect your bottom line.

Identity Theft Resource Center | https://www.idtheftcenter.org/
National non-profit that provides direct identity crime advice and resources.

Cyber Hawaii | https://www.cyberhawaii.org/resources/cyber-101/
Resources for small to medium size businesses to educate employees and build resilience against cyber attacks.

KEEP THIS INFORMATION READY BEFORE CALLING OR REPORTING

Incident details

- Date/time discovered and when payment/contact occurred
- Transaction amounts, account/payment details, destination information
- Names, phone numbers, emails, domains, usernames, and URLs involved

Evidence to preserve

- Original emails with headers if possible; texts/voicemails; screenshots
- Call logs, invoices, payment instructions, access logs, vendor communications
- Do not delete messages or wipe devices before preserving evidence

Important: Do not rely on caller ID, email display names, or links in a message. Independently verify using trusted contact information.

CENTRAL PACIFIC BANK

Member FDIC