



## **Impersonation Fraud: Internal Controls as Front Line**



**The Federal Trade Commission logged 2.6 million fraud reports in 2024, and reported losses exploded to a record \$12.5 billion - a 25% jump in just one year. Imposter scams topped the list again, generating over 845,000 reports and \$2.95 billion of losses. Those numbers underline a sober truth: accounting, finance, and operations teams are now on the front lines of a threat that has evolved far beyond clumsy phishing emails.**

## What Is Impersonation Fraud?

Impersonation fraud occurs when someone poses as a trusted party such as a vendor, a bank representative, a government official, or even a senior executive, and pressures an employee to transfer money, share credentials, or reveal sensitive data. These scams succeed because they prey on three human instincts: trust in familiar names, fear of urgent consequences, and a desire to comply quickly.

## How Technology Fuels the Threat

Technology now amplifies the danger. Artificial-intelligence tools can draft flawless emails, mimic corporate branding, and even generate a perfect replica of an executive's voice. Caller-ID spoofing makes any phone number appear legitimate. As a result, many of the old red flags, like poor grammar, awkward phrasing, or a foreign phone number, have all but disappeared.

## Technical Defenses

Because the threat straddles technology and human behavior, your defense must do the same.

On the technical side, verify that your company's email domains are protected by SPF, DKIM, and DMARC records. These will help prevent unauthorized third parties from sending email using your domain.



Multifactor authentication should be non-negotiable on email, online software, and banking platforms; it blocks intruders even when a password leaks.

Do not overlook the phone channel: register all outbound numbers with the free caller registry used by the major U.S. wireless carriers, and consider branded-calling or spoof-mitigation tools so customers and staff immediately recognize genuine company calls.

## Internal Controls and a Culture of Verification

Technology alone, however, will not close every gap. A disciplined control environment keeps employees from acting on fraudulent requests that slip past electronic filters.

Any change to vendor banking details, password reset, or wire transfer should require a second confirmation through a known phone number or an in-person conversation.

Payments above a preset dollar threshold ought to receive two approvals from different departments, and the power to create a new vendor should never reside with the same person who approves or releases payments.

Owners and CFOs can reinforce these standards by running unannounced spot checks of bank reconciliations and vendor-master records, a practice that both detects irregularities and signals vigilance.

Because most fraud is discovered internally, give employees a safe, anonymous way to raise concerns, whether that is a dedicated “security check” channel, a hotline, or a shared mailbox.

Finally, trade the once-a-year slide deck for short, scenario-based refreshers each quarter so staff learn to question requests that invoke secrecy, speed, or fear.



## Incident Response and Insurance

Preparation must also include a fallback plan. A crime or cyber-insurance policy that specifically covers social-engineering or funds-transfer fraud can limit the financial blow if an attacker slips through.

Equally important is an incident checklist: contact your bank immediately, freeze affected accounts, preserve evidence, and file a report at [ReportFraud.ftc.gov](https://www.ftc.gov/report-fraud). Fast action often determines whether funds can be recovered.

## External Audits and Continuous Improvement

External scrutiny brings an invaluable perspective. An annual engagement with a security or audit firm can include simulated phishing emails, fake vendor change requests, and a review of segregation of duties. That outside look exposes blind spots created by role drift or informal workarounds that accumulate over time.





# Next Step

Impersonation fraud is not merely an IT problem; it is a business-wide risk that demands coordinated defenses. Our firm can map your payment workflows, test approval paths, and help you embed practical controls without slowing daily operations. Please contact our firm if you would like to discuss your defences with one of our expert advisors. Together, we can strengthen the checkpoints that turn every employee—from the front desk to the C-suite—into an active part of the solution rather than the weakest link.

Ultimately, any request that arrives with a sudden deadline, threatens dire consequences, or introduces new payment instructions deserves scrutiny. Slow down, verify through a second channel, and remember that no legitimate partner will object to a double-check performed in the name of sound risk management.



## About Larson Gross

Ted Larson and Dennis Gross founded our firm in 1949. They built the business based on excellence, passion, integrity, trust and pro-action — values still important to us more than seven decades later.

Even well into their retirement years, Ted Larson and Dennis Gross continued to have the best interest of the firm at heart. Mr. Larson would come into the office on a regular basis to meet every new face and make a personal connection with each of our team members. He remembered the name of every employee, as well as the names of their spouses and children, and would greet clients by name as he passed by the reception desk. Sometimes, you'd even find a newspaper clipping on your desk that Mr. Larson dropped off, highlighting that your son made the honor roll. This is the example of a genuine relationship we strive to embody with our people and clients.

Today, we're led by ten partners who are growing our firm with respect for where we've come from and a new vision for future success. Our 120-plus team members and three offices located in Bellingham, Lynden and Burlington make us the 10th largest public accounting firm in the Puget Sound region. While we're determined to expand our impact and help strengthen as many businesses and individuals as we can, we're also committed to remaining a locally-owned organization. We're incredibly proud of where we've come from and look forward to a future of possibility



Larson Gross  
2211 Rimland Dr.  
Suite 422  
Bellingham, WA 98226



(800) 447-0177



[contact@larsongross.com](mailto:contact@larsongross.com)



<https://larsongross.com>

