ZURICH

Internet theft and fraud schemes

Please route to:

- Owner
- General manager
- Sales manager
- Service manager
- Office manager

Internet theft and fraud: Are you prepared?

Internet theft is an increasingly common crime and one that can present tremendous financial risk to your business. Two of the most frequent types of Internet theft affecting Zurich's customers are theft of vehicles and theft of parts.

To protect against these potential fraud schemes, dealerships should have strict identity verification safeguards in place for Internet customers, just as they would for customers who purchase in-person. Being thorough and consistent, and remaining diligent, are key to putting sufficient controls in place.

How does internet theft happen?

Two factors contribute to Internet theft at the dealership. First, the sense of urgency in making a sale can contribute to missing cues when information is provided by a thief. Second, in some cases, individual financial compensation can affect judgment when working through the sales process. This can be particularly common toward the end of the month or other contest periods, and thieves know this.

How is personal information fraudulently obtained?

Many businesses rely on easily obtainable personal information to approve sales. Most thieves steal the same, easily obtainable information through traditional and electronic methods.

Common traditional methods include:

- Bribery
- Burglary
- Credit card skimming
- Dumpster diving
- Shoulder surfing
- Stealing mail
- Stealing wallet
- Telephone scams
- Job-related

Common electronic methods include:

- Hacking
- Spyware
- Phishing
- Trojans/Viruses
- Fraudulent websites

Red Flags Rules

On January 1, 2011, the Federal Trade Commission (FTC) began enforcing its Fair and Accurate Credit Transactions Act of 2003 (FACT Act) Red Flags Rule. The Red Flags Rule requires that each "financial institution" or "creditor"—which includes most securities firms—implement a written program to detect, prevent and mitigate identity theft in connection with the opening or maintenance of "covered accounts." These include consumer accounts that permit multiple payments or transactions, such as a retail brokerage account, credit card account, margin account, checking or savings account or any other accounts with a reasonably foreseeable risk to customers or your firm from identity theft.[1]

Examples of red flags include unusual account activity, fraud alerts on a consumer report, or attempted use of suspicious account application documents. To be compliant, programs must be managed by a Board of Directors or senior employees and consist of six requirements: 1) Policy, 2) Training, 3) Detection, 4) Prevention, 5) Mitigation, and 6) Audit.

How prepared is your dealership?

To assess whether or not your business is prepared against Internet theft, ask yourself and your team the following questions:

- Have you evaluated the controls in place to prevent theft by those who have stolen another person's identity?
- Do you have a definitive identity verification process in place and is it followed by all employees?

- Who makes the decision to ship parts or roll vehicles when purchasing over the Internet?
- Are you in compliance with the Red Flag Rule?

What can you do?

Dealerships can protect themselves by taking these simple steps:

- Physically verify identification documents
- Remain diligent about looking for irregularities in customer information
- Fax checks to issuing banks for signature verification
- Use escrow service that is local to the buyer in Internet deliveries
- Utilize an Internet-based identity verification service
- Take a 'trust but verify' approach

Identity verification services

Zurich recommends the use of an Internet-based identity verification service. These services work by asking a "challenge" system of questions that require the customer to recall financial and other personal information up to 25 years old. The objective is to ask questions that can only be answered correctly by the true person alone. Identity verification services are convenient and effective for all types of sales transactions including in-person, phone, fax, and Internet.

Thieves continue to evolve in their knowledge of emerging theft methods and schemes. Internet theft and fraud are ever-present risks that all dealerships should address. The best protection is prevention, so controls should consistently be evaluated to help your dealership remain one step ahead.

Not a customer?

For more information about Zurich's products and Risk Engineering services, visit www.zurichna.com/automotive or call us at 800-840-8842 ext. 7449.

Already a customer?

Contact your Zurich Account Executive or agent for information about additional Zurich's products and Risk Engineering services.

Resources

1. FINRA.org https://www.finra.org/rules-guidance/key-topics/customer-information-protection/ftc-red-flags-rule#:~:text=The%20Red%20Flags%20Rule%20requires,accounts%20that%20permit%20multiple%20payments

The Zurich Services Corporation

Zurich Resilience Solutions I Risk Engineering

1299 Zurich Way, Schaumburg, IL 60196-1056

800 982-5964 www.zurichna.com

A1-P0380589-A (10/22) P0380589

ZURICH®
Resilience Solutions

Conclusion

Workplace violence is a major concern for businesses of all sizes, from large corporations to small family run businesses. Risk of violent acts and threats of violence can be reduced with the implementation of a comprehensive, written workplace violence prevention program. Violence prevention activities should become part of everyday work and management should remain vigilant in reviewing and sharing policies and resources with all employees on a regular basis.

Resources

1. https://www.osha.gov/sites/default/files/publications/osha3153.pdf
2. Society of Human Resource Managers https://www.shrm.org/ResourcesAndTools/hr-topics/employee-relations/Pages/Workplace-Violence-May-Jump-During-Return-to-Work.aspx

   https://www.shrm.org/hr-today/trends-and-forecasting/research-and-surveys/Documents/SHRM Workplace Violence 2019.pdf.
3. National Institute for Occupational Safety and Health (NIOSH)

The Zurich Services Corporation

Zurich Resilience Solutions I Risk Engineering

1299 Zurich Way, Schaumburg, IL 60196-1056

800 982-5964 www.zurichna.com

A1-P0340303-A (08/22) P0340303

ZURICH®
Resilience Solutions