Harland Clarke's integrated approach to keeping your account holders secure.

HARLAND CLARKE™

> “I’ve had my credit card re-issued for the second time this year. Why can’t companies keep my personal information secure?”
>
> *—Financial Institution Customer, Dallas, TX*

Security/fraud rank **#1** on the list of the banking industry’s top strategic initiatives.

Source: Financial Insights, Worldwide Banking 2007 Top 10 Strategic Initiatives: Finding New Strategies for Success, FIN205373, February 2007

Your account holders are concerned about their security.

Harland Clarke's *Integrated Security Process* provides coordinated practices and services that help mitigate their risk and your liability.

More than ever, your account holders are concerned about security. It's not surprising, given the challenges of securing data in an increasingly interconnected world. Reports of compromised customer or member or employee information are commonplace — as are e-mail scams, online phishing, spyware and computer viruses for home users.

Industry research shows that information security is a deciding factor when individuals choose a financial institution. Account holders expect their financial institutions to keep their personal information safe. If a breach of security should occur, the resulting loss in customer and member confidence and trust would be devastating for an institution's hard-earned reputation.

78%

of consumers feel that financial institutions are responsible for identity theft prevention.

Source: Unisys® white paper on identity theft prevention and detection, 2005

Solutions that work together to reduce risk.

To effectively address your account holders' security concerns, you need a comprehensive approach to security. Any one component of our Integrated Security Process can enhance your account holders' security; but, when used together, all components provide an exceptional level of protection from risk.

A deeply-embedded culture of security.

At Harland Clarke, we've maximized our expertise in quality practices into a superior system of corporate-wide security processes, as evidenced by receiving the Malcolm Baldrige National Quality Award in 2001 and our ongoing adherence to its policy. These include:

- Quality-control personnel who consider the impact of events such as equipment malfunctions and schedule changes not just on quality, but on security, as well
- A centralized security organization led by a Chief Security Officer and comprised of full-time, dedicated employees who oversee physical security, incident management, internal/external audits, regulatory compliance, account holder privacy, and data security
- Extensive background checks and drug testing of new employees
- Annual security and ethics training for all new and current employees

Security training.

Training your personnel can play a key role in making your customers or members more secure. A staff trained in security is not only more likely to be able to identify fraud, but is better able to speak knowledgeably on the subject with your account holders. That's why we offer an **Identity Theft Awareness Course** free of charge to financial institution employees. It's one of many online courses pertaining to security that we offer as part of our Online University program.

Secure marketing services.

Our contact center and direct mail marketing services are an ideal choice for conveying marketing messages to your customers and members. By partnering with us for these services, you can reduce the number of companies with which you share your customers' data, thereby reducing your risk. Our contact center personnel undergo the same rigorous screening as our other employees, and they are trained to deal with suspicious activity and resolve fraudulent activity.

Security expertise that meets the challenge of emerging threats.

Working closely with financial institutions gives our security team an industry-wide view on risks in a constantly changing environment.

In addition to serving thousands of financial institutions, our security team actively participates in governmental and industry security initiatives.
Our team also partners with other leaders in security including VeriSign®, Cybertrust® and IBM®, to stay on top of emerging threats.

Relationships maintained by our security team include:

- USPS Inspector General's Task Force
- Postal Inspectors Committee
- National Academy Associates (an organization of local, state and international law enforcement officials who are graduates of the FBI Academy)
- Direct contact with FBI Cyber Units, the FBI Lab and the FBI Fraud Group
- Ongoing meetings with security counterparts in the shipping industry, including the United States Postal Service®, DHL®, UPS® and FedEx®
- InfraGard® (a nationwide communications network on terrorism and other types of criminal activities and frauds)
- Annual Terrorism Symposium
- Panels with U.S. Secret Service and FBI

"I found no critical issues and assessed that Harland Clarke had a well-documented, mature security program, and that the processes supporting the program were sound."

—Client quote at completion of security audit (October 2007)

Helping financial institutions comply with FACT Act ruling.

Effective November 1, 2008, financial institutions must comply with federal regulations designed to curb identity theft. **The Fair and Accurate Credit Transactions (FACT) Act** requires financial institutions to adopt a written identity theft prevention program to protect account holder information. By partnering with Harland Clarke, our security processes, experience and wide range of account holder security offerings will become integral to your identity theft prevention program.

When *CSO* magazine looked at financial services security, they looked to us.

What they found was a company that had successfully built upon its background in a security-related business by evolving its nationally acknowledged expertise in quality control processes into an expertise in security processes. Quoting from the article:

The three top priorities of the new security program, [John] Petrie [Harland Clarke's Chief Security Officer] says, included taking advantage of enterprisewide quality processes (the company won a Malcolm Baldrige National Quality Award in 2001); linking security and risk mitigation decision processes to the business's operating plan and strategic growth goals; and ingraining security into the mind-set and daily activities of Harland Clarke's employees. "We wanted to make sure security wasn't a thing that sits out there and functions on its own," Petrie says.

Source: October 2007 CSO magazine case study. (CSO is the preeminent trade publication for business risk leadership)

"We rely on Harland Clarke to provide best-in-class services to our customers, while always making us look good."

—Financial institution officer, quoted from a recent brand survey

Collaborative services for communicating securely.

Secure marketing and contact center services.

As a security partner already entrusted with your account holders' non-public information, we're the natural choice for communicating with your account holders by phone and mail. Our direct mail and call center personnel undergo the same extensive background screening as our other employees. Our representatives are specially trained to speak with confidence about financial services issues, to identify fraudulent activity and professionally address your account holders' security concerns.

Our capabilities include:

- Outbound phone and credit card activation and deactivation support and overflow-call assistance in the event of an unplanned volume surge
- Direct mail operations that can provide personalized documents and inform your customers about your privacy policy, a new product or a security incident

Marketing Services direct mail certification.

Harland Clarke's industry-standard security extends to all aspects of our contact with your customers. Our Marketing Services' production facility is one of the few in the industry that has successfully met the stringent security requirements for Payment Card Industry (PCI) compliance, as of November 2007.

Complimentary Identity Theft Awareness Course.

Make our complimentary Identity Theft Awareness Course a key part of your security program. It is self-directed, multimedia-based, and employs audio, video, animation, interactivity, and proven adult-learning techniques that can promote a greater retention of course information by your employees. The course discusses ways to identify and prevent theft before it can hurt your account holders. It also identifies the common methods criminals use to obtain personal information such as mail theft, 'dumpster diving', and 'pharming', along with ways to address these risks.

Learn more about accessing this training from your account executive or by going online to:

www.harlandclarke.com/security

The Integrated Security Process: a holi

Because a security process is only as safe as its most vulnerable link, Harland Clarke utilizes an integrated approach to security that considers every point of potential risk for you and your account holders. This total approach — what we call our *Integrated Security Process* — makes us a leader in secure solutions.

In addition to embedded solutions, we offer an array of products and services that enhance the security you can offer your customers. These deeper layers of security, including authenticated, online check ordering, undeliverable (non-forwarded) mail handling and trackable delivery, provide additional defense against identity fraud.

A three-part process for maximum protection.

Our corporate-wide, multi-layered, defense-in-depth security process is comprised of three parts that work together to shield your account holders from harm across a range of contingencies:

- **Fraud Prevention** confirms caller and online identities, validates incoming account data and offers products with specially designed paper stocks and high-security inks
- **Identity Protection** safeguards non-public information and helps secure shipment of orders
- **Identity Recovery** assists victims of theft in recovering their identities

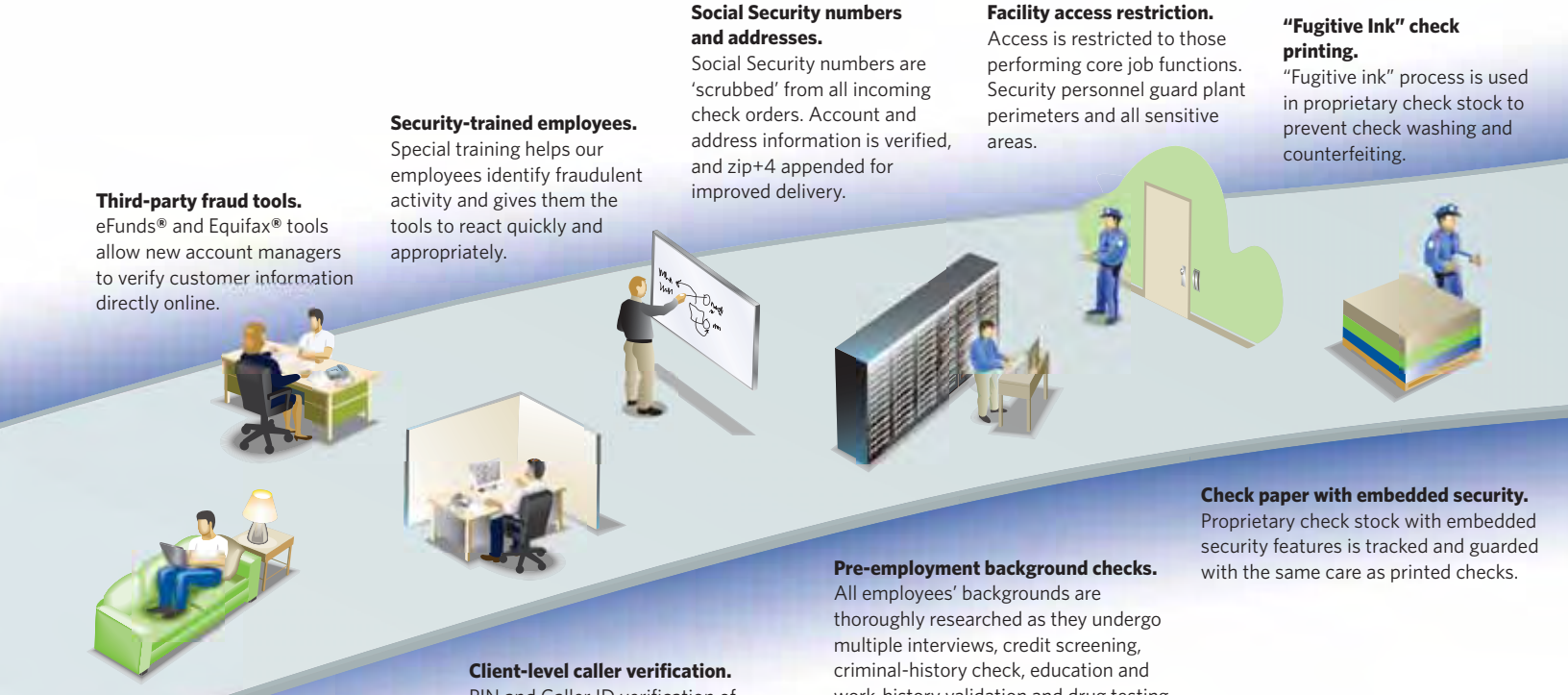
Third-party fraud tools.
eFunds® and Equifax® tools allow new account managers to verify customer information directly online.

Security-trained employees.
Special training helps our employees identify fraudulent activity and gives them the tools to react quickly and appropriately.

Social Security numbers and addresses.
Social Security numbers are 'scrubbed' from all incoming check orders. Account and address information is verified, and zip+4 appended for improved delivery.

Facility access restriction.
Access is restricted to those performing core job functions. Security personnel guard plant perimeters and all sensitive areas.

"Fugitive Ink" check printing.
"Fugitive ink" process is used in proprietary check stock to prevent check washing and counterfeiting.



Check paper with embedded security.
Proprietary check stock with embedded security features is tracked and guarded with the same care as printed checks.

Pre-employment background checks.
All employees' backgrounds are thoroughly researched as they undergo multiple interviews, credit screening, criminal-history check, education and work-history validation and drug testing.

Client-level caller verification.
PIN and Caller ID verification of incoming branch calls helps prevent impersonation of employees and ordering by unauthorized individuals.

VeriSign® Cybertrust® audit and SSL encryption.
128-bit SSL encryption ensures orders placed online are transmitted securely. They are then audited by VeriSign and Cybertrust.

stic approach to mitigating risk.

A standards-based and certified process.

In order to maximize the reliability and security of different sub-processes, we follow these accepted best practices and industry standards:

- ISO Standard 17799/27001: Code of Practice for Information Security Management covering authentication, encryption, vulnerability testing, monitoring, and annual auditing
- National Institute of Standards and Technology (NIST) 800 Series guidelines
- Federal Financial Institutions Examinations Council (FFIEC) guidelines
- Control objectives for Information and Related Technology (CobIT®) guidelines
- IBM's GSD331 standards for secure server environments
- Internal audits to assess the handling of secure/sensitive data as it relates to Sarbanes-Oxley and Gramm-Leach-Bliley compliance, as well as the Statement on Auditing Standards No. 70

Incident Management and Protection.

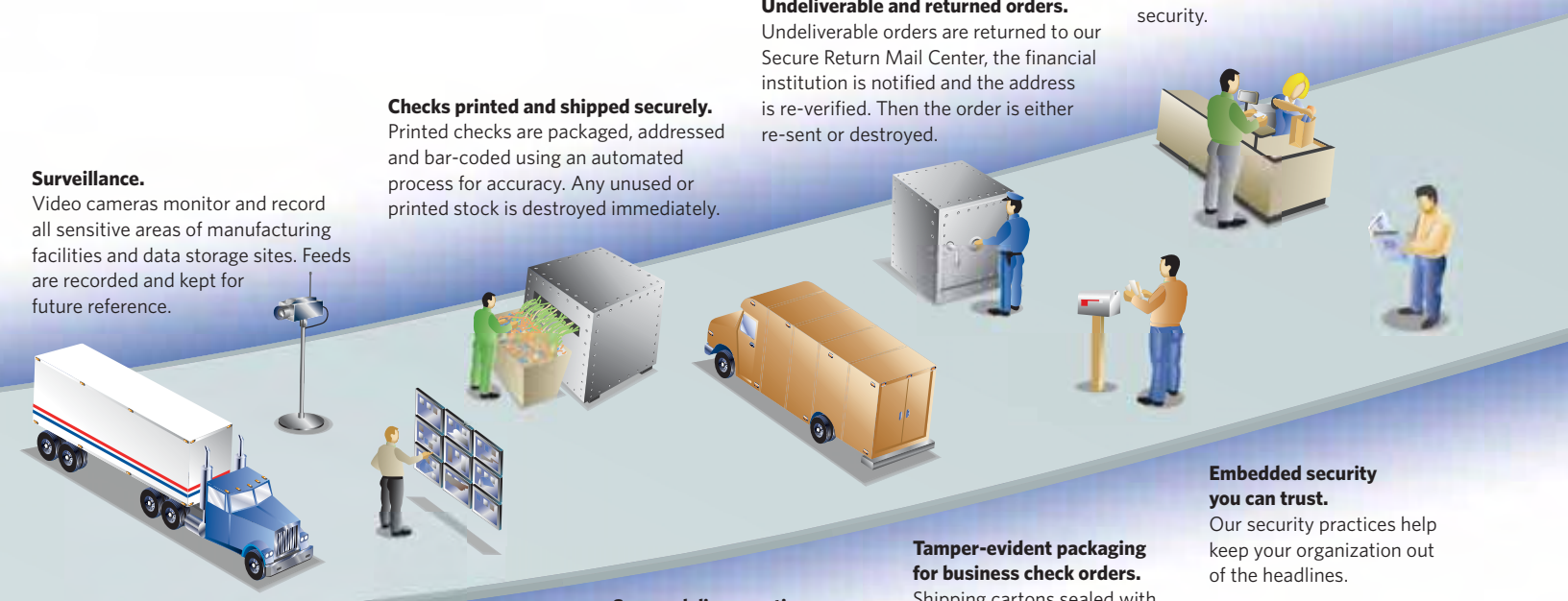
Harland Clarke has contingency plans and system redundancies, practiced and in place, to respond to almost any level of disaster. Our Corporate Business Continuity Plan (CBCP) and Disaster Recovery Plan (DRP) are tested and reviewed annually by executive management and updated as critical changes occur.

Fraud-deterrent products.
Special pens with wash-resistant ink that can help prevent identity theft are available for enhanced account holder security.

Undeliverable and returned orders.
Undeliverable orders are returned to our Secure Return Mail Center, the financial institution is notified and the address is re-verified. Then the order is either re-sent or destroyed.

Checks printed and shipped securely.
Printed checks are packaged, addressed and bar-coded using an automated process for accuracy. Any unused or printed stock is destroyed immediately.

Surveillance.
Video cameras monitor and record all sensitive areas of manufacturing facilities and data storage sites. Feeds are recorded and kept for future reference.



Embedded security you can trust.
Our security practices help keep your organization out of the headlines.

Tamper-evident packaging for business check orders.
Shipping cartons sealed with nylon-reinforced security tape and tamper-evident inner bags protect the integrity of the entire business check order.

Secure delivery options.
Economical, trackable delivery options are available to all consumer and business check buyers to ensure their orders can be located during shipment.

Fraud risks are mitigated.
Investigation units monitor and adjust processes to ensure that risk is mitigated. Should an incident occur, response teams communicate with customers immediately.

Secure-supplier practices.
Secure vendor practices, including yearly audit, maximize end-to-end security.

Business check order security enhancements.

We also offer enhanced security measures for businesses that reduce the risk of theft during the check-order fulfillment process. They include:

- Guidance during ordering by business product experts
- Screening of orders and phone numbers for potential fraud
- Shipping of check orders in tamper-evident packaging
- Team of investigators to review potential fraudulent check orders

Our Integrated Security Process is a dynamic, interconnected system of operations and practices designed to mitigate risk and respond to emerging trends in a constantly evolving business environment.

To learn more about the benefits of partnering with a leader in industry security, contact your Harland Clarke Account Executive today or write to us at www.harlandclarke.com/contactus.

HARLAND CLARKE

10931 Laureate Drive
San Antonio, Texas 78249
Tel: 210 697 8888
Fax: 210 696 1676
www.harlandclarke.com

SAMM 9102360