Healthcare Industry Wisdom on

Medical Identity Fraud

Executive Summary

November 2016

Industry Wisdom on Medical Identity Theft and Fraud

The Medical Identity Fraud Alliance (MIFA) has collected "industry wisdom" from a variety of sources to help healthcare organizations navigate their medical identity theft and fraud prevention, detection and mitigation efforts. The full version of the Wisdom Paper is available on the MIFA website, http://medidfraud.org/resources/publications/.

Medical identity fraud is the fastest-growing identity fraud, affecting more than two million people annually in the United States.[1] It is growing in volume, impact, and financial cost and the implications can be life-threatening. Medical identity theft and fraud are not bound by geography, income or other demographics. The crime and its victims can be found distributed across the U.S. and throughout all areas of the healthcare industry.

There is no silver bullet to preventing fraud and no one-size-fits-all solution. However, with careful recognition of each area of risk and how best to mitigate those risks, the healthcare industry can reduce the incidence of medical identity theft and fraud, and therefore reduce the harmful consequences to victims and to the industry. Each type of healthcare organization must evaluate their individual risks − both overall as an enterprise organization and individually in each area of their business − and then choose protocols, processes, technologies and other available means that are deemed appropriate for each situation.

A Growing Concern

Medical identity fraud is defined as when someone uses an individual's name and other personally identifiable information (PII) and/or protected health information (PHI) to fraudulently receive medical services, prescription drugs and/or healthcare goods. It also includes using false identities for fraudulent healthcare billing.

The *Fifth Annual Study on Medical Identity Theft*, conducted by the Ponemon Institute and sponsored by the Medical Identity Fraud Alliance (MIFA) and its members, show a year-over-year increase of nearly 22 percent in medical identity fraud, producing almost half a million more victims in 2014 than in 2013. At the five-year anniversary of this study, research indicates the occurrence of medical identity theft incidents has almost doubled in those years.[2]

Convergence of Market Drivers for Criminals

Healthcare providers and health plans are top targets for identity theft since they hold rich stores of consumer data, including health plan numbers, social security numbers, dates of birth and other sensitive details in medical records. The shift to electronic health records (EHRs) since the

[1] *Fifth Annual Study on Medical Identity Theft*, http://medidfraud.org/2014-fifth-annual-study-on-medical-identity-theft/, Medical Identity Fraud Alliance (MIFA), February 2015.
[2] *Fifth Annual Study on Medical Identity Theft*.

2009 Health Information Technology for Economic and Clinical Health (HITECH) Act, while improving information sharing and enabling better care delivery, has created a lucrative environment for cyber criminals.

PHI is extremely profitable on the black market, creating demand for healthcare-related identity data. Cyber attackers are receiving considerably more on the black market for healthcare credentials compared to stolen credit card numbers.[3] Health record data is more valuable since it can contain both traditional personally identifiable information (PII), financial data and PHI, all in one location. This information can be exploited in a variety of identity frauds.

Medical identity fraud can take much longer to detect than other types of identity fraud. Further, data points in PHI, such as a birthday or social security number, cannot be "closed" and reissued after its been compromised, unlike bank or credit account numbers. Because of these converging factors, criminals can often perpetrate the fraud over a long period of time.

Consequences of Medical Identity Fraud

The implications are far reaching, resulting in an average $13,500 out-of-pocket cost to the victim[4], in addition to many other headaches associated with identity theft. Unlike financial identity fraud, there are currently no similar legal or regulatory consumer protections in place that limit the financial liabilities. The Fair Credit Billing Act, which limits the identity theft victim's fraud losses to fifty dollars, does not apply in medical identity fraud situations (it would only apply if the identity thief paid for medical goods or services with a fraudulent credit card). Therefore, the victim may struggle with remediating an unlimited amount of financial fraud losses created by the identity thief.

Not only can identity fraud ruin the victim's credit when bills remain unpaid, but inaccurate medical records created by the fraudster can threaten the victim's future care and health. False claims could exhaust the maximum limits of the victim's health plan, precluding coverage in the event of a medical emergency. Theft of patients' identity data also poses credit risk outside the healthcare system, where criminals can use stolen social security number and date of birth to apply for loans or credit cards.

Victims of medical identity fraud may suffer damaging reputational consequences when sensitive medical or health information is publicly disclosed. The disclosed information may be true information about the victim which they wish to remain confidential, or it may be incorrect, damaging information about the identity thief, which is now attributed to the victim in their medical records. Most victims indicate suffering embarrassment and/or reputational consequences.[5] A few victims also suffer negative employment issues, such as job loss, lost advancement opportunities or loss of a professional license. This may occur when the victim's employment is conditioned upon certain health-related conditions, such as being drug-free. For example, if the identity thief has a drug abuse problem, that information is now in the victim's health record, potentially jeopardizing the victim's employment.

---

[3] http://www.fortherecordmag.com/archives/0316p18.shtml.

[4] *Fifth Annual Study on Medical Identity Theft*.

[5] *Fifth Annual Study on Medical Identity Theft*.

The most threatening consequences are the potential ramifications to the victim's health. Consequences can include misdiagnosis, mistreatment, delay in receiving proper care, being prescribed the wrong medication and permanent or long-lasting errors to medical records. Medical records may become corrupted with information from the identity thief, creating unsafe healthcare situations for victims when there is confusion about the victim's true health status. Possible negative health outcomes may include the victim receiving medication to which he or she is allergic, or scenarios such as a diabetic not receiving the proper care because her health record does not reflect her disease.

A large number of medical identity theft victims know the perpetrator. In 25 percent of cases, the "victim" was complicit in the fraud, willingly providing their health identity information to someone else for fraudulent use.[6] This often is the situation when individuals loan their medical credentials to uninsured relatives and friends who need medical services. Those who do this may be unaware of the risks of sharing this type of personal information, particularly what can happen when their medical record becomes co-mingled with that of the person with whom they are sharing medical identities.

Medical identity theft and related PHI data loss also have an impact on the healthcare industry, not just on consumers who've been victimized. Studies indicate those whose identity information has been lost or otherwise breached by a healthcare organization are more likely to switch providers or health plans.[7] In addition to the cost to remediate any data theft/loss, the reputational costs to an institution can have lasting effects.

The number of healthcare organizations plagued by negative headlines has led to heightened patient sensitivity about sharing their personal information. Sixty-four percent of patients cite privacy issues as a key concern for accessing health information online and another 21 percent admit to withholding information from doctors out of concern of data security.[8]

Understanding the increased threat to our healthcare data is important, but so are finding resources and tools to mitigate these risks. Recent big healthcare data breaches have increased the healthcare industry's awareness of the growing threats to patient data and privacy. With this new awareness comes increased scrutiny of how health care organizations are protecting individual consumers.

If patients and health care organizations work together to prevent and identify fraud when it occurs, we will be in a much more solid position to defeat those who wish to perpetrate identity crimes—saving both money and lives.

The full paper, Healthcare Industry Wisdom on Medical Identity Fraud, is available on the MIFA website

---

[6] *Fifth Annual Study on Medical Identity Theft*.
[7] *Fifth Annual Study on Medical Identity Theft*.
[8] *Fifth Annual Study on Medical Identity Theft*.

About the Medical Identity Fraud Alliance (MIFA)

MIFA is an industry trade association of healthcare providers, payers and stakeholders, working to help our members better protect consumers from medical identity theft and the resulting fraud. MIFA members provide leadership to mobilize the healthcare ecosystem; cooperate to leverage collective intellectual capital and power; research to adequately understand the problem and guide solution building; educate consumers, industry, legislators and regulators; and empower individuals to be the first line of defense in protecting their Protected Health Information (PHI). Our goal is to reduce the frequency and impact of medical identity fraud, through work such as research, public-private collaboration and information sharing. For more information visit http://medidfraud.org/.

MIFA Members and Strategic Partners

AARP *

Aetna

SPHER, Inc.

Association of Credit Counseling Professionals *

BlueCross BlueShield Association *

CareFirst BlueCross BlueShield

Center for Identity Management and Information Protection-Utica College *

Clearwater Compliance, LLC

Coalition Against Insurance Fraud *

Consumer Federation of America *

CSID

Experian

Florida Blue

Generali Global Assistance

Henry Ford Health System

ID Experts Corporation

Identity Fraud Institute at Hodges University

Identity Guard/Intersections, Inc.

Identity Theft Resource Center *

IDology, Inc.

Information Systems Security Association – South Florida Chapter *

Kaiser Permanente

LifeMed ID, Inc.

Maryland Crime Victims Resource Center *

National Health Care Anti-Fraud Association *

Northwell Health

Secure ID Coalition *

Smart Card Alliance *

Stoel Rives

UnitedHealthcare

U.S. Department of Labor *

U.S. Department of Veterans Affairs *

* Strategic Partner

Resource Appendix

Use of these resources is the responsibility of the user. The following list is offered as an educational resource by MIFA members, reflecting their diverse expertise in preventing, detecting and mitigating medical identity theft and fraud, and the effects on the victim and the healthcare industry.

Center for Identity Management and Information Protection (CIMIP)

Identity Theft Victim's Resources
http://www.utica.edu/academic/institutes/cimip/idcrimes/resources.cfm

New Study Finds Companies at Risk for Fraud
Protiviti, Utica College Survey Finds Lack of Proactive Fraud Risk Management Poses Significant Risk to Corporations. Majority of companies not prepared to conduct investigations, study finds
http://www.utica.edu/academic/institutes/cimip/mediacenter/index.cfm?action=detail&id=4318

Utica College/CIMIP Releases Report: "New Face of Identity Theft"
Offenders Older, Acting in Groups, Targeting Strangers
http://www.utica.edu/academic/institutes/cimip/mediacenter/index.cfm?action=detail&id=4305

Hiding in Plain Sight
Funded by a grant from the Bureau of Justice Assistance, this project is an examination of characteristics of identity manipulation performed by sex offenders to obfuscate their own identities. The report also provides recommendations on how to effectively address this problem.
http://www.utica.edu/academic/institutes/cimip/publications/index.cfm?action=submit

Identity Fraud Trends and Patterns: Building a Data-Based Foundation for Proactive Enforcement
Funded by a grant from the Bureau of Justice Assistance, this project is an assessment of closed United States Secret Service cases which have an identity theft/fraud component.
http://www.utica.edu/academic/institutes/cimip/publications/index.cfm?action=submit

Consumer Federation of American (CFA)

My company's had a data breach, now what? 7 questions to ask when considering identity theft services
When companies, organizations or government agencies experience a data breach that may have exposed people's personal information, one of the many issues they must address is how to help those affected. Consumer Federation of America and its Identity Theft Service Best Practices Working Group, which includes consumer advocates and identity theft service providers, have created a checklist explaining the different kinds of monitoring and fraud resolution that may be offered. http://consumerfed.org/wp-content/uploads/2016/09/9-7-16-7-Questions-to-Ask_Fact-Sheet.pdf.

Experian Data Breach Resolution

When a data breach hits, one wrong maneuver can put you in the path of fines, litigation, customer turnover and brand erosion. Experian Data Breach Resolution upholds the highest standards of regulation and compliance to bring you premium data breach resolution. We'll meet your needs for effective and fast resolution, and we'll help protect the individuals looking to you for added security following a data loss. We customize and scale our services to discreetly handle each breach of data, whether it affects hundreds, thousands or millions of individuals. From notification to fraud resolution, we offer superior support for you and your customers during a data breach. http://www.experian.com/data-breach/data-breach-resources.html

Generali Global Assistance

Before the Aftermath: The Importance of Identity Protection in the Age of the Data Breach
Data breaches can leave behind a path of destruction that lasts for years, sometimes forever, and credit monitoring alone fails to effectively secure personally identifiable information (PII) in the aftermath. This whitepaper describes how to secure the best identity protection to minimize risk after your data has been exposed. http://generaliga.hs-sites.com/before-the-aftermath-the-importance-of-identity-protection-in-the-age-of-the-data-breach

ID Theft Toolkit
There were over 13 million victims of identity theft in 2015. Smart thieves are using new and increasingly convincing social engineering tactics to obtain the confidential information they need to steal identities. This infographic highlights some of lesser known but still very common tactics criminals are using to access data and how you and your customers can avoid becoming their next victims. http://irisidentityprotection.com/articles/identity-theft-toolkit-infographic/

Iris Products. Iris brings together a powerful combination of advanced identity monitoring technology and award-winning resolution for 360° protection that minimizes the risk of identity theft.
Iris Enterprise Solutions
Iris Online Data Protection Suite
(See attached sheets for Iris product information)

ID Experts Corporation

MIDAS: Medical Identity Alert System. MIDAS is an innovative healthcare fraud solution from ID Experts, developed to lower healthcare costs and protect consumers' medical identities through early detection and prevention of healthcare fraud. (See attached sheet for MIDAS product information)

IDology, Inc.

Identity Verification Solutions:
Identity Verification. IDology's ExpectID solution helps verify identity for account onboarding and user access.
Age Verification. ExpectID Age allows users to verify age of patients ordering age-restricted items online.
Authentication. IDology' ExpectID IQ is a dynamic knowledge-based authentication solution that helps with password resets and higher levels of identity verification.
Photo ID Verification. ExpectID Scan Verify and Scan Onboard allows you to bring identity verification to a higher level by scanning and verifying a user's ID or passport or to quickly onboard new customers at check in.

White Papers:
Security and Authentication in Healthcare: A Mercator Advisory Executive Group Brief Sponsored by IDology
Mercator Advisory Group recently interviewed fraud management executives at healthcare organizations to evaluate the risks and challenges posed in the healthcare sector by identity theft originating online or from mobile devices. These executives head fraud management or patient information privacy compliance functions within healthcare provider organizations, insurers, or healthcare payment networks. Conclusions drawn from these interviews are summarized in this Executive Brief.

Improving Patient Portal Adoption and Decreasing Fraud with Advanced Identity Verification Solutions
This white paper examines practices that enable healthcare organizations to deliver enhanced identity verification practices that provide a more convenient and less intrusive experience for end users accessing healthcare information exchanges.

Iris.On Watch.

Your partner in people-first identity protection.

Provided by Generali Global Assistance, Inc.

Iris brings together a powerful combination of advanced identity monitoring technology and award-winning resolution for 360° protection that minimizes the risk of identity theft.

Identity Monitoring

Iris scours the deepest corners of the Internet, searching for compromised credentials and potentially damaging use of personal information, detecting fraud at its inception.

Credit Monitoring

Iris enables easy access to credit scores and credit reports to ensure accuracy of credit profiles.

Suspicious Activity Alerts

At the first sign of suspicious activity, Iris will send an alert that includes how to take action and prevent damage.

Iris watches for:

- Changes to credit profile
- High risk transactions
- Compromised credentials
- Black market activity
- New payday loans
- Telecom accounts opened

Resolution Support

Iris provides 24/7 support from an award-winning team of certified identity theft resolution specialists with the expertise to handle complex issues and situations.

Iris provides a personal case manager to help with:

- Affidavit submission
- Creditor notification and follow-up
- Communications with law enforcement
- Credit freezes
- Lost wallet assistance
- Fraud alerts
- Emergency cash and travel arrangements

Digital Privacy Protection

Keep personal information secure with a downloadable suite of privacy protection software designed to prevent hackers and malicious websites from stealing data.

Online Dashboard

Iris provides a dashboard to easily monitor identity risk level, track credit profiles, access identity theft protection tips and respond to suspicious activity alerts from one place.

$1 Million Identity Theft Insurance

In the event of theft, Iris provides reimbursement for out-of-pocket expenses related to the recovery process.

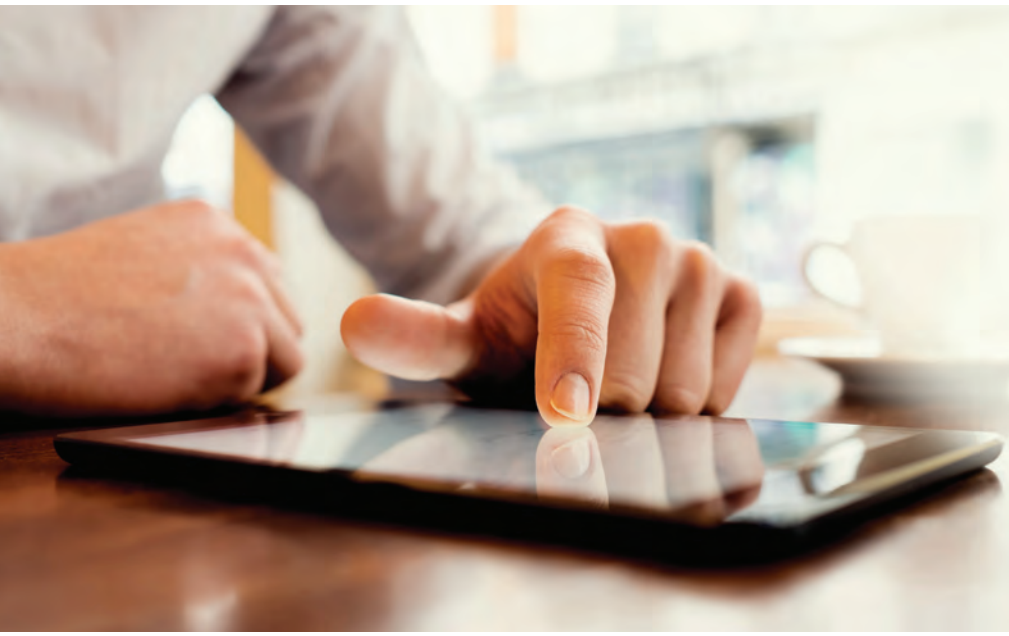
Generali Global Assistance (GGA), formerly Europ Assistance in the U.S., is based in Bethesda, Maryland, and has been a leader in the assistance industry since its founding in 1963. Generali Global Assistance is a division of the multinational Generali Group which in 185 years has built a presence in more than 60 countries with more than 76,000 employees. GGA was one of the first companies to provide identity theft resolution services in the U.S. and today is a provider of identity protection services to leading companies, proudly protecting millions of customers.

For more information contact iris@us.generaliglobalassistance.com or visit www.irisonwatch.com to request a demo.

GENERALI GLOBAL ASSISTANCE

*Identity Theft Insurance underwritten by Generali U.S. Branch. This summary is intended for informational purposes only and does not include all terms, conditions and exclusions of the policy. Coverage may not be available in all jurisdictions. Please refer to the actual policy for terms, conditions, and exclusions of coverage. Generali U.S. Branch (New York, NY; NAIC # 11231) operates under the following names: Generali Assicurazioni Generali (U.S. Branch) in California, Assicurazioni Generali – U.S. Branch in Colorado, Generali U.S. Branch DBA The Generali Insurance Company of Trieste & Venice in Oregon, and The Generali Insurance Company of Trieste and Venice – U.S. Branch in Virginia. Generali U.S. Branch is admitted or licensed to do business in all states and the District of Columbia.

Iris™ On watch.™



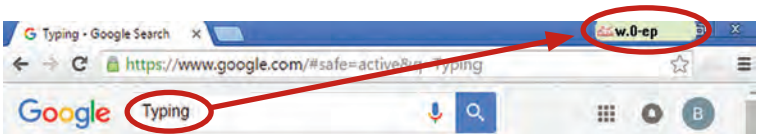
Online Data Protection Suite

Protect Sensitive Data from Cybercriminals

There were over one million web attacks launched every day in 2015.[1] With Iris' Online Data Protection software, you can use the internet without worry. A key component of Iris' 360° approach to identity protection, Online Data Protection helps defend against keylogging and phishing attacks – going beyond standard anti-virus software.

Traditional anti-virus programs are designed to protect computers from virus attacks. Our Online Data Protection Suite, comprised of DataScrambler® and PhishBlock®, is designed to also protect user data which helps combat 50 % of new malware that conventional solutions fail to detect. The Iris Online Data Protection Suite file – less than 1MB – is easily downloaded and installed in three clicks, taking less than 30 seconds.

DATASCRAMBLER®



DataScrambler® is inserted into a user's browser and shows the actual keystrokes being replaced by alternate keystrokes, providing a visual display of how the user's information is being continuously protected. The anti-keylogging technology used in DataScrambler® operates at multiple levels, using specialized techniques that thwart attackers from stealing data entered by a user. Attackers see scrambled data rather than the customer's real data.

PHISHBLOCK®

PhishBlock® uses proactive and customized anti-phishing technology to detect malicious websites designed to steal user information the very first time they are loaded. The technology is "trained" via proprietary methods to identify phishing sites of all major brands targeted by attackers. PhishBlock® automatically identifies scam sites that have been newly published – even before traditional anti-virus programs classify them as known phishing sites – and overlays a warning page to inform the user.

GENERALI GLOBAL ASSISTANCE

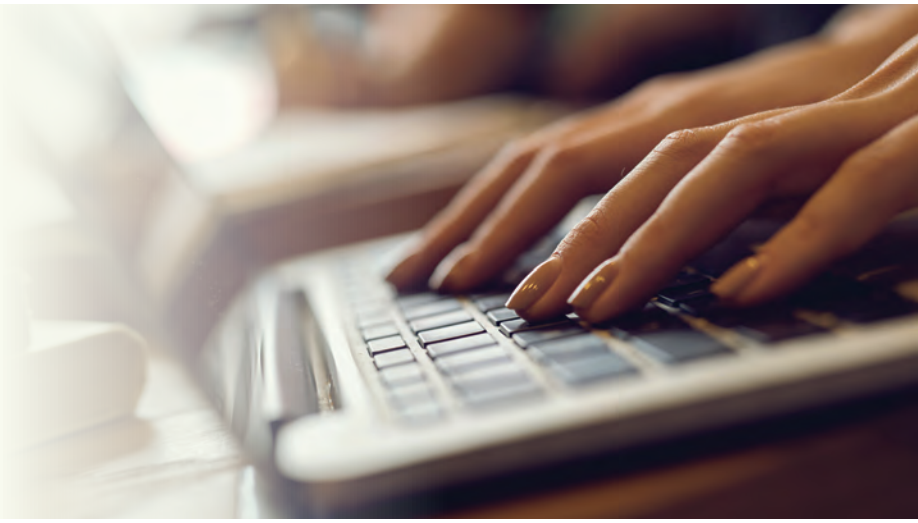
IRIS OFFERS IDENTITY PROTECTION IN FOUR STEPS

Prevention

Monitoring

Alerts

Resolution



THE CYBERCRIME PROBLEM

- The number of phishing sites **increased from 24,864 to 33,571** between 2014 and 2015[2]
- Cybersecurity incidents have **surged 38%** since 2014[3]
- **44%** of U.S. millennials have become victims of online crime in the last year[4]
- **Four in five** people worry about becoming a victim of online crime[3]
- **27%** of all recorded malware appeared in 2015[5]
- **204 million** cyberattacks were recorded around the world in 2015[6]
- **27%** of internet users who report using free public Wi-Fi say they used it to access their banking account or purchase a product with a credit card[7]

STRENGTHEN DIGITAL SECURITY WITH IRIS' ONLINE DATA PROTECTION SUITE

- Protect every keystroke users type (identity information including passwords, credit card numbers, etc.)
- Prevent screenshot malware that captures images of user data
- Prevent users from being lured to a fake (phishing) site where their data can be stolen
- Show every keystroke users type as being scrambled and protected
- View a monthly report showing what data has been protected

BENEFITS OF IRIS' ONLINE DATA PROTECTION SUITE

CONSUMER BENEFITS

- Multiple layers of protection outperform all other major desktop security packages in thwarting new spyware attacks
- DataScrambler® and PhishBlock® do not need to identify threats to prevent data theft
- Protection is automatic, invisible, and simple to use – no change in user habits is required

BUSINESS PARTNER BENEFITS

- A timely and unique product feature with broad customer appeal and relevance to everyday life and habits
- Proactive protection customers can see working – visible and persistent presence on users' desktops shows they are being protected each time they use the internet

Sources: 1. Symantec, Internet Security Threat Report, Volume 21, April 2016. 2. Google Security update – 2015 I/O Conference 3. PWC - The Global State of Information Security Survey 2016. 4. Norton Cybersecurity Insights Report. 5. https://heimdalsecurity.com/blog/10-surprising-cyber-security-facts-that-may-affect-your-online-safety/. 6. Convenience Versus Security: Challenges of a Wireless World, AARP, July 2015. 7. Convenience Versus Security: Challenges of a Wireless World, AARP, July 2015

For more information contact ***iris@us.generaliglobalassistance.com*** or visit ***www.irisonwatch.com***

GENERALI GLOBAL ASSISTANCE


Iris™
On watch.™
Meet Iris,
Your Identity
Protection Partner.

Iris is people-first identity protection by Generali Global Assistance.

Iris puts your customers in control of their identity with a 360° approach to identity protection that includes:

» advanced identity monitoring

» suspicious activity alerts

» award-winning resolution services

» an easy-to-use online dashboard

Iris' many features can be customized to create a program that best fits your customers' needs.

PROTECT YOUR CUSTOMERS AND GROW YOUR BUSINESS WITH IRIS

People are turning to the businesses and organizations they trust to provide the peace of mind that comes from having comprehensive identity protection.

In today's competitive business environment, the need to stand out is greater than ever. New product offerings can help companies reinforce brand value while attracting and retaining customers.

Identity theft is one of the fastest growing crimes in America. **Offering identity protection makes good business sense: it's a hassle-free way to create an additional revenue stream, engage customers and build brand loyalty.**

There is a new victim of identity theft **every three seconds**

50% **More than half of victims spend over a year trying to resolve the issue and are often harassed by debt collectors and/or denied credit**

A survey of victims found that...

65% **feel rage or anger**

40% **report sleep disturbances**

28% **are unable to concentrate**

22% **still have collection agencies calling**

SOURCES:
Javelin Strategy & Research, Identity Theft Resource Center

YOUR PARTNER IN IDENTITY PROTECTION

Generali Global Assistance has decades of expertise protecting millions of identities and has earned the trust of leading Fortune 500 companies.

Partnering with Generali Global Assistance provides your customers with the protection they need while positioning you as a market leader. Our commitment is to your success. Iris' flexible identity protection programs are designed to meet your business needs, offering:

- **Voluntary or embedded programs**, seamlessly integrated into your business' product, package and portfolio
- **Customizable individual, couple and family plans** to meet your customers' needs
- **Rapid implementation and hassle-free administration**
- Choice of **white label, co-branded or Generali Global Assistance branded platform** and materials
- **Marketing and messaging support** to drive engagement
- **Dedicated account management** to assist with set-up, roll out and maintenance

Iris provides 360° identity protection for your customers in four steps:

PREVENTION

Defend personal information and enhance privacy.

24/7 Expertise & Online Resources – access to Iris' certified identity theft resolution experts and online educational resources

Opt-out Services – reduce pre-approved credit card offers, direct mail campaigns and marketing phone calls that thieves can use to steal your information

Online Data Protection Software – guard against keylogging and phishing, two common ways hackers steal personal information

MONITORING

Track identity risk level and detect potential fraud early.

Online Dashboard – easily monitor identity risk levels, track credit profiles, access identity theft protection tips and respond to alerts from one place

Advanced Identity Monitoring – fraud is detected at its inception as Iris scours the deepest corners of the Internet to search for compromised credentials and potentially damaging use of personal information

Credit Monitoring – access credit reports and scores to ensure accuracy of credit profile

ALERTS

See suspicious activity and take action immediately.

Alerts are sent if Iris detects:

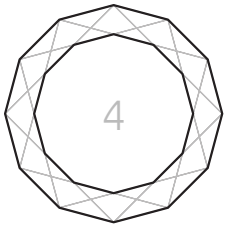
» Changes to credit profile

» High-risk transactions

» Compromised credentials

» Black market activity

» New payday loans



While many companies focus on data protection alone, Iris is dedicated to the well-being of the person behind the data. Generali Global Assistance's award-winning identity protection team goes above and beyond to ensure that the recovery process is as quick and easy as possible.

RESOLUTION

Resolve problems quickly and easily with help from Iris' experts.

Iris' certified identity resolution experts are available 24/7 to handle complex issues and help with:

» Affidavit submission

» Creditor notification and follow-up

» Communications with law enforcement

» Credit freezes

» Lost wallet assistance

» Fraud alert placement

» Emergency cash and travel arrangements

» Translation services

» Financial and legal counseling

» IRS identity theft services

» Stress management

$1 Million Identity Theft Insurance* for recovery expense reimbursement

*Identity Theft Insurance underwritten by Generali U.S. Branch. This summary is intended for informational purposes only and does not include all terms, conditions and exclusions of the policy. Coverage may not be available in all jurisdictions. Please refer to the actual policy for terms, conditions, and exclusions of coverage. Generali U.S. Branch (New York, NY; NAIC # 11231) operates under the following names: Generali Assicurazioni Generali (U.S. Branch) in California, Assicurazioni Generali – U.S. Branch in Colorado, Generali U.S. Branch DBA The General Insurance Company of Trieste & Venice in Oregon, and The General Insurance Company of Trieste and Venice – U.S. Branch in Virginia. Generali U.S. Branch is admitted or licensed to do business in all states and the District of Columbia.

For more information, contact
iris@us.generaliglobalassistance.com
or visit www.irisonwatch.com

ABOUT GENERALI GLOBAL ASSISTANCE, INC.

While you may not be familiar with GGA, we've been here all along. We've been busy protecting clients and their employees for over 50 years. As the pioneer of the assistance concept, we have decades of knowledge and perspective that comes from working with a diverse array of industries. The result is customized, innovative services to help our clients grow and retain business. GGA was one of the first companies to provide identity theft resolution services in the U.S. and today we are a leading provider of identity protection services, proudly protecting millions of employees from the growing threat of identity theft. Identity theft knows no bounds or geographical limits. Neither does GGA's global reach or expertise. We stand ready to provide hands-on assistance to minimize the distress employees face when confronted with identity fraud, wherever life takes them.

GGA, formerly Europ Assistance in the U.S., is based in Bethesda, MD, and has been a leader in the assistance industry since its founding in 1963. GGA is a division of the multinational Generali Group which, over 185 years, has created a presence in more than 60 countries with over 78,000 employees. Our success has been built upon the foundation of trust that clients have placed in our ability to provide assistance in the most difficult of circumstances. **Customer service is not just a philosophy – it's our culture. We endeavor to exemplify our mission as your trusted partner in identity protection.**

midas

PRODUCT DATASHEET

Engaging members to fight healthcare fraud

MIDAS: Medical Identity Alert System

MIDAS is an innovative healthcare fraud solution from ID Experts, developed to lower healthcare costs and protect consumers' medical identities through early detection and prevention of healthcare fraud.

At a glance:

- MIDAS is "alert driven"
- Engages and empowers health plan members
- Monitors for medical identity theft and fraud
- Meets key compliance components of the Affordable Care Act
- Applies proven fraud reduction strategies from financial services
- Simple to use, simple for members to understand, and secure
- Provides members with dispute resolution
- Lowers healthcare costs

A new healthcare fraud solution for health plans

MIDAS—Medical Identity Alert System—the newest software solution from ID Experts, aims to engage health plan members to monitor their health care transactions and take control of their medical identity.

The result is lower healthcare costs; early identification of healthcare fraud; timely monitoring against the possibility of medical identity theft; and enhanced resolution of fraud issues. Engaging members, (patients) throughout the healthcare process is a key compliance component of the Affordable Care Act.

Healthcare fraud & theft: A growing problem

MIDAS was developed to help fight against the escalating costs and risks associated with healthcare fraud and medical identity theft.; Medical identity theft has affected 2.32 million victims according to the 2015 Survey on Medical Identity Theft; and as millions more Americans enter the healthcare insurance market under the Affordable Care Act, fraud and abuse are expected to escalate. records are breached

MIDAS helps individuals get ahead of fraud

Today, the misuse of medical indentities is typically discovered long after medical records have been compromised, and after providers have been paid. MIDAS helps the consumer to identify and investigate suspicious claims much earlier in the payment process—streamlining the fraud and medical identity theft investigation process and leveraging ID Experts proven expertise in dispute resolution—so that the breached individuals and the health plan can reduce fraud losses and lower their costs.

Learn more at:
www.IDExpertsCorp.com/MIDAS

MIDAS engages individuals as first line of defense

MIDAS uses smartphone text and emails to alert members when a healthcare transaction is submitted, leading the member to a secure site that displays summary information in plain language. The member can then validate the transaction or mark it as "suspicious."

If suspicious, a fraud alert notifies the MIDAS team for prompt follow-up. If fraud or medical identity theft has indeed occurred, MIDAS leverages ID Experts' proven resolution processes to diagnose the problem, resolve the issue, and mitigate any harm.

MIDAS is designed to compliment payers' existing systems and is highly configurable.

MIDAS simplifies medical transactions

According to the 2013 Survey on Medical Identity Theft, 54 percent of consumers do not currently check their health records and EOBs for inaccuracies because they either don't know how or say it's too difficult. Of those who found unfamiliar claims, 52 percent did not report them. MIDAS is the first and only healthcare fraud solution that engages members to monitor their healthcare transactions and take control of their medical identities.

MIDAS makes this easy by communicating to members in plain language, so they can quickly review and approve claims, before they are paid. This will help payers to identity healthcare fraud and medical identity theft early, reduce fraud losses, and reinforce their commitment to engaging and protecting members.

MIDAS is fast for payers to integrate

MIDAS works in tandem with the payer's existing claims system and is designed to be a "plug and play" implementation. Additionally, the MIDAS solution is agnostic, fully encrypted and supports payer privacy and security initiatives.

Board of Advisors

- **James Christiansen**, Chief Information Risk Officer, RiskyData, Former identity theft program manager, FTC
- **Gary Gordon**, Ed.D., Partner, Bluewater International
- **Deborah Peel**, M.D., Founder, Patient Privacy Rights
- **Jim Pyles, Esq.**, Principal, Power, Pyles, Sutter & Verville PC
- **Larry W. Walker**, President, The Walker Company
- **Norm Willox**, Managing Partner, Bluewater International, Former CEO Lexis Nexis

1

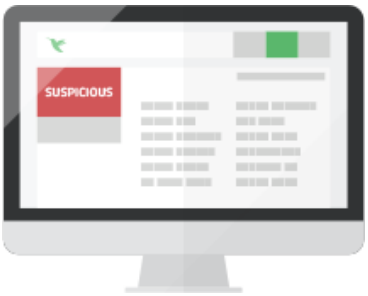
Medical Activity Alert Deployed

MIDAS provides timely text messages or emails to alert members anytime a claim is made against their medical identity.

2

Consumer Reviews

MIDAS' mobile-friendly application securely displays claim information in simple language and without messy paperwork.



3

Confirm or Mark as Suspicious

Upon reviewing those claims, members can identify possible fraud, billing errors, even medical identity theft, and can securely notify the MIDAS team for prompt follow-up.

4

Fraud Investigated & Resolved

If fraud or medical identity theft has occurred, MIDAS leverages ID Experts' proven dispute resolution processes to diagnose the problem, resolve the issue, and mitigate any harm.

Talk to a MIDAS expert

866-534-7455 | midas@IDExpertsCorp.com

id experts®

About ID Experts

At ID Experts, we provide innovative software and services that help organizations manage the risks of data incident response and identity fraud. Our MIDAS software received the 2014 Gartner Cool Vendor award for insurance payers. Insurers use MIDAS to engage their members as the first line of defense in reducing fraud and preventing medical identity theft.

Lenovo Health AIMe, Powered By LifeMed ID

A universal patient identity solution.

What are the biggest health IT risks you face?

Most care organizations have found duplicate records, medical identity theft, and payment fraud to be one of their biggest health IT challenges—contributing to revenue loss, medical errors, and patient dissatisfaction.

Duplicate Records
skew patient population metrics and put patients at risk for medical errors and inappropriate treatment.

- On average, an excess of 10% of medical records are duplicates, per facility/network

Medical Identity Theft
compromises patient health data and patient safety

- Over 2 million medical identity theft victims—paying about $13,500 each to resolve
- National damages of up to $84 billion a year

Payment Fraud
is a major factor in revenue loss ... tens of billions in revenue loss.

- $272 billion is lost to healthcare fraud and abuse within Medicare and Medicaid programs alone
- In 2015, the Department of Justice sanctioned more than $1.9 billion from civil healthcare fraud cases

Key business benefits of Lenovo Health AIMe

Improve organizational efficiency and care delivery for better patient outcomes with Lenovo Health AIMe. Only Lenovo Health AIMe can offer you:

Accuracy
100% Verified Patient Identity
- Ensure quality of patient data for better clinical decisions
- Limits the opportunity for medical identity theft or fraud

Knowledge
Real Patient Population Metrics
- Accurately identify the health of your active patient population and assess the impact of care improvement efforts
- Improve patient outcomes and appropriate care delivery

Savings
Better patient outcomes and streamlined billing
- Increase reimbursement
- Enhance revenue cycle integrity and reduce liabilities held in annual revenue
- Reduce money and time spent on fraud reconciliation
- Simplify payment collection
  —Access all pending/outstanding account activity at check-in

How it works

Validate
a patient's identity, address, and active insurance information—100% accurate identity verification

Implement
the leading authoritative identity management solution to optimize workflow and reduce risks

Connect
a patient to an ID token and automatically invoke his or her electronic health record across your network

Connect an ecosystem of secure, reliable devices—from tablets to servers—with Lenovo Health AIMe to automate workflow from the point of admission.
For more information, visit lenovohealth.com/patient-id/

Lenovo Health
Customized care, anywhere
www.lenovohealth.com