Protecting Patient Information

Balancing Security & Patient Experience
About IDology

- IDology provides innovative technology solutions that verify an individual’s identity and/or age for organizations operating in a customer-not-present environment. The IDology platform serves as a collaborative hub for monitoring and stopping fraudulent activity across the entire network while also driving revenue, decreasing costs and meeting compliance regulations.

- Founded in 2003, IDology offers a solution-driven approach to identity verification and fraud prevention, providing streamlined processes that ultimately help increase customer acquisition and improve the overall customer experience. IDology has developed an on-demand technology platform that allows customers to control the entire proofing process and provides the flexibility to make configuration changes that are deployed automatically – without having to rely on internal IT resources or IDology’s customer service – so customers can stay ahead of the fraud landscape while also maintaining compliance.
IDology for Healthcare

Identity for the Healthcare Industry

- Assists healthcare organizations with verifying patient and provider identities
- Helps meet compliance regulations
- Prevents fraud at all touchpoints - online, call centers and mobile
Protecting Patient Information While Balancing Security & Patient Experience

Challenges & Opportunities:

• Multiple Fraud Threats
  • Data Breaches
  • New Mobile Channels
  • BYOD – Bring Your Own Device

• Increased Awareness

• Emerging Investments in IDV and Fraud Management
# Data Breaches and Social Engineering

## Top 10 Healthcare Data Breaches 2015

<table>
<thead>
<tr>
<th>Organization</th>
<th>Records Breached</th>
<th>Type of Breach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anthem</td>
<td>78,800,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>PREMERA BLUE CROSS</td>
<td>11,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>Excellus</td>
<td>10,000,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>UCLA Health</td>
<td>4,500,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>MIE Medical Informatics Engineering</td>
<td>3,900,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>CareFirst</td>
<td>1,100,000</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>DMAS</td>
<td>697,586</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>Georgia Department of Community Health</td>
<td>557,779</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>BEACON Health System</td>
<td>306,789</td>
<td>Hacking / IT Incident</td>
</tr>
<tr>
<td>DJO Global</td>
<td>160,000</td>
<td>Laptop Theft</td>
</tr>
</tbody>
</table>

| 2015 Total              | 111,022,154      | (almost 35% U.S. population) |

The Economics of the Black Market for Healthcare Data Illustrates the Value of Stealing More Information

A partial EHR can be sold for up to $50 versus $1 for a stolen credit card or social security number.

Complete healthcare information with other documents can command up to $1,000. Healthcare insurance information alone is worth $20 each.

Bulk medical records were reported to be sold for $6.40 for each record.

Identity Theft Has Less To Do With Payments-related Data Breaches and More About Diving Deeper into Relationships

Higher value data resides where consumer/business relationship is deeper and more personal and fraudsters can take over accounts.

Source: Identity Theft Resource Center Summary as of 9/29/2015
Survey: Healthcare

In 2015, IDology sponsored a primary survey consisting of first-person interviews with executives across a range of industries. These interviews were designed to gain a deeper understanding of the fraud and risk management dynamics in these segments.
Key Findings: Healthcare

1. Online medical records can be accessed by a variety of individuals, based on need, and through various portals – complicating the risk environment.

2. Portal account registration and other patient-related functions (like billpay) are managed through different portals. Most of the investments in fraud technologies are made in the account registration infrastructure.

3. Data encryption and multi-factor authentication processes were often in place to check the identities of healthcare providers or practitioners accessing their systems.
Survey: Brand Impact and Increased Mobile Usage Drive Risk Management Concerns

“... We strongly believe that the extra finances and effort in dealing with preventive measures for fraud and compliance is minimal compared to the expense of dealing with the harm to our consumers and the organization, the brand damage that occurs in putting out the fires when an organization is faced with fraud and breaches.”

Chief Privacy Officer, healthcare provider

“Within the next five years, we expect more mobile hacks to occur. As organizations become more mobile, you always need to improve your identity verification and fraud management capabilities. There is always an opportunity for improvement, so we will be investing every year in this area as new techniques arise. Authenticating the user is more challenging, even if password based. We must continually invest in our fraud management capabilities to add multiple layers of active defense.”

Chief Technology Officer, healthcare payments network
A Quickly Expanding Security Agenda

• Traditionally, healthcare organizations have focused on meeting compliance

• The new era of patient portals and online data accessibility

• Many realize that current measures are insufficient in today's online and mobile age
Today’s Digital Reality

• The emergence of patients and providers utilizing mobile devices

• Growing need for mobile-optimized identity verification and fraud prevention platforms

• Criminals find lucrative opportunities in healthcare

• Organizations must continually adapt to shifting fraud patterns
Challenges of Mobile

- Nearly 41% of American homes are wireless only
- Consumers and physicians are now accessing medical records on mobile devices
- Authenticating a device can be laborious and may not persist through change events
Multiple Fraud Threats - BYOD

• Using personal mobile devices for work has given rise to a trend called “Bring Your Own Devices” or BYOD

• More and more mobile devices are an avenue to breach an organization

• Possible threats of BYOD for healthcare organizations:
  • Data leakage
  • Malware
  • Account Takeovers
Emerging Investments in IDV and Fraud Management

• What's important to protecting patient information?
  • Access Management
  • Layered Fraud Prevention
  • Device Identity and Attributes

• A layered approach to fraud prevention and access management is critical

• Authentication is a critical concern

• Providers and healthcare organizations must balance the patient experience with security
Taking the Friction Out of Authentication Requires Rapid, Contextual and Flexible Workflows

Knowledge-based authentication workflows can pull friction out of the authentication process and harden data security by providing deeper context and decision reliability.

This is especially important when data is being accessed by multiple users for myriad use cases making access to rich, contextual data more important.
Key Takeaways

• Organized fraud is both dynamic and opportunistic and will always migrate to the weakest point not only within a stakeholder, but at the market level whenever new products are introduced. When opportunity is turned off in one channel or for one product, the criminal will search for the next entry point.

• As more transaction activity moves to digital and mobile channels, service providers have to find the means to balance user experience with risk management and design their risk management strategies with the user experience in mind.

• The availability of multiple layers of authentication data and information, combined with step-up algorithms will be increasingly leveraged in order to balance cost, experience, and risk.
Questions?

Kevan Sears
Enterprise Sales
ksears@IDology.com
678.324.3788

Christina Luttrell
SVP, Product Management
cluttrell@idology.com
https://www.IDology.com